

Facing the Camera

Good Practice and Guidance for the Police Use of Overt Surveillance Camera Systems Incorporating Facial Recognition Technology to Locate Persons on a Watchlist, in Public Places in England & Wales.

The Protection of Freedoms Act 2012 & The Surveillance Camera Code of Practice.

Issued by the Surveillance Camera Commissioner

By virtue of Section 34(2)(c) Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice.

Published: November 2020





Foreword



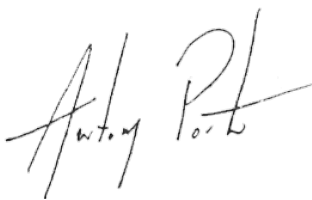
In the context of state surveillance, live facial recognition technology (LFR) is but a single modality example of a new and innovative genre of surveillance platforms. Its use by the police in England and Wales thus far serves to illustrate a much wider challenge facing society in my view, namely the creation and modernisation of rules and safeguards which inform, constrain and hold to account the overt use of increasingly sophisticated and available surveillance technologies by law enforcement agencies. The Court of Appeal adjudicating in the case of *R(Bridges) v The Chief Constable of South Wales Police* applied valuable judicial scrutiny to such matters. I was a contributor to those particular proceedings and I commend both Liberty and South Wales Police for their respective contributions which brought about and enabled the court process to provide direction, which will benefit future law makers, decision takers and the public alike. I have taken that judgement in to account amongst other factors in revising my guidance, which seeks to provide a road map through the complex terrain which must be navigated if this this technology is to be used legitimately and in a manner which inspires public confidence.

As the independent regulator of the overt use of surveillance cameras in public spaces by the police in England and Wales, my role is unique in a western democracy. I am fortunate in being supported by a broad spectrum of incredibly talented specialist individuals and organisations who give so generously of their expertise in support of my regulatory role. I am very grateful to them and others who have contributed to this publication. I am clear in my view that the police should have recourse to the tools necessary to keep us safe, including facial recognition technology in appropriate circumstances. The technology unquestionably has the potential to help the police keep communities safe from harm yet its use is intrusive. I still believe that there remains a degree of opaqueness as to the current legal framework which accommodates LFR use by the police which would benefit from a revision of legislation, the Secretary of State's Surveillance Camera Code of Practice (SC Code) and regulatory safeguards.

Hence, my revised guidance, which seeks to add value to the high level standards which the government expects of operators of public space surveillance camera systems as is set out in the SC Code. My guidance is simply that, guidance and not law, as to those matters which I consider important and helpful for Chief Officers, Police and Crime Commissioners and the wider public to consider where the use of this technology is being considered with regard to the SC Code. I have no regulatory powers beyond that. My guidance goes beyond the strict requirements of the law in suggesting what I consider to be good practice and is significantly more detailed than its previous iteration; "The Police Use of Automated Facial Recognition Technology used with Surveillance Camera Systems" which I published in March 2019, and deliberately so. It arises from seven years pedigree of my regulatory function and from the expert contributions of those who support me both inside and beyond the National Surveillance Camera Strategy. It is intentional on my part that my guidance begins with sections which relate to the inherent considerations applicable to issues of 'equality' and 'ethics'

before turning to the statutory, regulatory and good practice considerations. I feel that this is the obvious chronology where the use of this technology is being considered to protect the public against threat and risk. The content of this document relates to the use of LFR in 'live time' and 'near real time' circumstances. It is not intended to relate to specific tactics, methodologies or other biometric applications which are used beyond a surveillance camera system. It is my hope that the production of this revised document will assist police decision makers and the wider public as to the issues and standards applicable to the use of this technology and to those who scrutinise such use. Police and Crime Commissioners have such an important role as the democratically elected voice of communities who both enable and hold Chief Officers to account. It is my sincere hope that my guidance will be of some value to those who are charged with the difficult task of determining future statutory and regulatory provision. Throughout the content of my guidance I make a number of good practice recommendations for practitioners to consider at a tactical/operational level, these will be found in the body of the guidance text. I also offer up a number of higher level strategic recommendations for senior stakeholders. None of those recommendations are in any way binding. They are for others to consider as they see fit and are summarised at the end of the document within its annexes.

No matter how energised the pace of statutory and regulatory evolution may or may not be, such progress can never hope to match the speed of capability evolution of algorithms and the inherent intrusion risk they increasingly represent to our civil liberties. I strongly believe that the modernisation and application of high level and clear legal principles and safeguards, the integrity, transparency and accountability of endeavour by our police, and a better informed public are amongst key ingredients which will help get ahead of the questions posed by evolving surveillance and other biometric capabilities, and thereby bring the future, and the answers necessary for our democratic society to truly benefit from surveillance camera technologies, in to a far sharper focus.

A handwritten signature in black ink, appearing to read 'Antony Porter'. The signature is fluid and cursive, with the first name 'Antony' written in a larger, more prominent script than the last name 'Porter'.

Antony Porter
Surveillance Camera Commissioner

IMPORTANT NOTICES

- I. This guidance is produced by the Surveillance Camera Commissioner (the SCC) to assist police forces in England and Wales to comply with their statutory obligations arising from Section 33 Protection of Freedoms Act 2012 (PoFA) and the Surveillance Camera Code of Practice (SC Code). This publication has been prepared to assist in the considerations which are to be applied by police forces who are operating or intending to operate overt surveillance camera systems in public places in England and Wales together with facial recognition technology to locate persons who are on watchlist. The guidance is to be read in conjunction with the SC Code. It does not effect changes to that Code.
- II. For the purpose of this document the term LFR (“live time” facial recognition) is used throughout its content and should be interpreted by the reader as referring to the “live time” and “near real time” operation of facial recognition technology where it is operated as part of a surveillance camera system as described at Section 29(6) Protection of Freedoms Act 2012 (PoFA).
- III. The SCC provides this guidance by virtue Section 34(2)(c) PoFA and in consideration of paragraph 5.6 of the SC Code which is as follows:

“The commissioner should provide advice and information to the public and system operators about the effective, appropriate, proportionate and transparent use of surveillance camera systems and should consider how best to make that information available. Such advice should complement the content of this code, and may for example provide additional detail on good practice, advice on the effectiveness of surveillance cameras and how this might be assessed, or on the proportionate application of any new technological developments in surveillance camera systems. Such advice could, for example, include the preparation of a manual of regulation that sets out how the commissioner will fulfil his functions.”

- IV. The content of this guidance is only applicable to Chief Officers and Police and Crime Commissioners of police forces in England and Wales. Any reference to ‘the police,’ ‘police forces,’ ‘Chief Officers’ or ‘Police and Crime Commissioners’ etc. within these contents are to be regarded accordingly.

R(Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058

- V. The SCC has revised his previous guidance, “The Police Use of Automated Facial Recognition Technology used with Surveillance Camera Systems” which he issued in March 2019, and in doing so takes in to consideration the recent judgement delivered by the Court of Appeal in the case of R(Bridges) v The Chief Constable of South Wales Police (the Bridges case). This guidance also takes into account the combined learning and experience derived from the National Surveillance Camera Strategy (NSCS), the work of the Commissioner’s Independent Advisory Group (IAG), the operational experience of the police, the stakeholder network which supports and informs the Commissioner and the wider statutory framework applicable to the conduct of police

surveillance which is signposted in the SC Code, including the Common Law, PoFA, the Data Protection Act 2018, the provisions of the Regulation of Investigatory Powers Act 2000 and attendant code of practice for Covert Surveillance and Property Interference, the policies provided by the police and other informed commentary from organisations and individuals.

- VI. It is important to note that in reaching its decisions in the Bridges case, the Court of Appeal accepted the submission of the SCC that the court was only concerned with the deployment of LFR by South Wales Police in the particular circumstances before it and was not concerned with the possible use of LFR by the police in the future on a national basis.
- VII. The Judgement delivered by the Court of Appeal in that case is fundamentally important for police forces who are considering the use of LFR. The interpretation of any aspect of that particular Judgement is a matter for Chief Officers where they seek to rely upon it in whole or in part, in the context of any future conduct they are considering which makes use of LFR. In such matters they are urged to consult with their legal advisers as they consider to be necessary. The SCC does not offer an interpretation as to any aspect of the Bridges case. A copy of the relevant Judgement is accessible at the below link;

<https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf>

The Surveillance Camera Commissioner

- VIII. The Surveillance Camera Commissioner is appointed by the Secretary of State by virtue of Section 34(1) Protection of Freedoms Act 2012. The Commissioner is independent of Government and has the following statutory functions provided at Section 34(2):
- (a) encouraging compliance with the Surveillance Camera Code,
 - (b) reviewing the operation of the code, and
 - (c) providing advice about the Code (including changes to it or breaches of it)
- IX. The SCC is not a judicial authority. The good practice guidance set out within this document is the regulatory opinion of the SCC which in suggesting good practice goes beyond the strict requirements of the law. It simply indicates the way in which the Commissioner is minded to construe the statutory provisions arising from PoFA and those within the SC Code which the SCC feels may be helpful to police forces intending to use or deploy LFR as part of their surveillance activities. The provisions of this guidance also apply to the use of surveillance camera systems owned or operated by third party organisations and operators, from both the public and private sectors, where such systems are being operated in partnership with, or at the behest of the police. The SCC has no powers of inspection, audit or sanction. His regulatory role is one of advice, encouragement and support. The SCC does not give legal advice or qualified legal opinion and nothing within this document should be construed or otherwise interpreted as amounting to being such.

SCC Guidance and the Surveillance Camera Code of Practice

- X. The SC Code is produced by the Secretary of State and not the SCC. It provides the standard which the Government expects of relevant authorities (including the police) who operate **overt surveillance camera systems** in **public places** in England and Wales. This guidance is provided to assist those seeking to comply with the SC Code. This guidance does not replace or effect any changes whatsoever to the contents of the SC Code. (Definitions of the terms in bold above are provided at paragraph 1.1 SC Code).
- XI. Wherever police forces consider operating LFR the SCC strongly encourages them to seek their own legal guidance before doing so.
- XII. ‘Golden threads’ which run through this guidance include the importance of Chief Officers seeking legal advice as to their conduct using LFR, the creation of suitably specific, safeguards which are applicable to the exercise of police discretion, (particularly in respect of those decisions as to who is to be placed upon a watchlist to have their whereabouts located by means of LFR and where such conduct is to take place), the importance of equality, transparency and accountability for decision making which should be based upon reasonable grounds, and the importance of producing publicly accessible policies which explain the safeguards to be applied in the context of the law, with due regard given to confidentiality.
- XIII. This guidance replaces the previous guidance issued by the SCC (“The Police Use of Automated Facial Recognition Technology used with Surveillance Camera Systems”) in its entirety. It is recommended that Chief Officers of police forces and Senior Responsible Officers who are appointed by the Chief Officer to oversee compliance with PoFA and the SC Code have their own personal copy of this revised guidance.
- XIV. The Surveillance Camera Commissioner’s office can be contacted at the following email address: scc@scccommissioner.gov.uk

Relevant Public Commentary by the Surveillance Camera Commissioner

“I have often stated that the public do not expect an analogue police force in a digital age but they have every right to expect clear, transparent and common-sense laws and rules to govern police conduct and use of those technologies – as indeed do the police themselves.”

Blog: “The Debate on Automatic Facial Recognition Continues” – 21.3.19

<https://videosurveillance.blog.gov.uk/2019/03/21/the-debate-on-automatic-facial-recognition-continues/>

“To be clear, I am and always have been strongly of the view that the police should have the tools they need to keep us safe. We have the best police in the world committed to do the right things in the right way. For me there is no question on that point. In the context of cameras, citizens and the state need the confidence in clear laws and regulation which proportionately enables the ethical use of technologies and holds such use to account now, and in the future. I continue to bang the drum on both points until the very end.”

Blog: “A farewell – Looking back to the future through the camera lens (Part 1)” – 19.2.20

<https://videosurveillance.blog.gov.uk/2020/02/19/a-farewell-looking-back-to-the-future-through-the-camera-lens-part-1/>

“The use of AFR will continue to dominate the public attention and focus. The ever-increasing use of AFR in the private sector will continue to be a concern. The increasing use between the private sector and the State is also of concern. In line with my guidance to police forces, I will continue to argue as follows:

- Consult your solicitor before proceeding.
- Consult your authorising officer under RIPA to ensure that legislation does not apply.
- Justify and risk assess your intended use of the technology.
- Engage your community and be transparent in its operation.
- Keep an exhaustive audit trail of your policies and documents.
- Consult my office to ensure compliance with PoFA.
- Consult your Data Protection Officer to ensure compliance with DPA and refer to ICO if necessary.

One thing is certain, existing surveillance laws will continue to be challenged as technical capabilities grow and State compulsion to use them grows. However, it remains incumbent upon the State to demonstrate that they are operating ethically and in accordance with the laws that govern such use,...

Annual Report 2018 – Surveillance Camera Commissioner

<https://www.gov.uk/government/publications/surveillance-camera-commissioner-annual-report-2018-to-2019>

Further details of the SCC’s public “Blog” commentary may be found on the Commissioner’s web site at the following link: <https://videosurveillance.blog.gov.uk>

Table of Contents

| | |
|--|----|
| 1. Applicability of Guidance | 12 |
| 2. Biometrics, Equality and Ethics | 14 |
| Biometrics and LFR | 14 |
| The Public Sector Equality Duty (PSED) | 15 |
| Ethics | 18 |
| 3. Human Rights, 'In Accordance with the Law' and The Legal Framework | 20 |
| Human Rights | 20 |
| In Accordance with the Law | 21 |
| The Legal Framework | 22 |
| The Common Law | 22 |
| The Data Protection Act 2018 | 23 |
| The Protection of Freedoms Act 2012 (PoFA) | 24 |
| The Surveillance Camera Code of Practice | 25 |
| Police Policy Documents – Legitimacy and Specificity (The 5WH) | 27 |
| The Regulation of Investigatory Powers Act 2000 and Overt Surveillance Camera Systems | 31 |
| Necessity | 33 |
| Proportionality | 34 |
| Risk Assessment | 35 |
| 4. Governance, Approval, Watchlists, Protected Characteristics and the Human Decision Maker | 37 |
| Governance | 37 |
| Senior Responsible Officer | 38 |
| Approval | 39 |
| Use of Images and Watchlists – The 'Who' question | 41 |
| Considerations regarding Subjects | 42 |
| Considerations regarding the Images | 44 |
| Protected Characteristics – Race and Gender | 45 |
| Protected Characteristics – Children, Missing and Vulnerable Persons | 45 |
| Protected Characteristics – Ageing and Facial Changes | 46 |
| Protected Characteristics – People with Disability | 46 |
| Face Coverings | 46 |
| Information Gathering and Persons of Specific Police Interest | 47 |
| Intelligence | 48 |
| Other Considerations | 48 |
| Human Decision Making | 49 |
| Similarity Threshold | 51 |
| Statutory Collaborations | 52 |
| Partnerships and the use of Third Party Owned/Operated Systems | 52 |
| Operational Trials | 54 |

| | |
|---|----|
| 5. Integrity, Use of Material as Evidence and Handling of Material | 55 |
| Digital Integrity and Forensic Standards | 55 |
| Evidence | 55 |
| Handling of Material | 57 |
| 6. Public Engagement, Provision of Information, Performance | 58 |
| Public Engagement | 58 |
| Provision of Information | 58 |
| Performance Management | 59 |
| “False Positives and Negatives” | 60 |
| 7. Accountability and Certification | 63 |
| Accountability | 63 |
| Certification | 64 |
| Annex A – Summary List of Recommendations | 65 |
| Annex B – Guiding Principles of SC Code | 68 |
| Annex C – Forensic Science Regulators approach to validation | 69 |

1. Applicability of Guidance

- 1.1. The Surveillance Camera Code of Practice is issued by the Secretary of State and regulated by the Surveillance Camera Commissioner under the provisions of the Protection of Freedoms Act 2012 (PoFA). Chief Officers of police forces in England and Wales (s33(5)(j)) and their Police and Crime Commissioners (s33(5)(h)), are 'relevant authorities' as prescribed by s33(5) PoFA (the Mayor's Office in London s33(5)(g)) and are therefore bound by a duty to have regard to the guidance within the SC Code when deploying a surveillance camera system to observe in a public place, as part of their functions. The duty to have regard to the SC Code includes the operation of surveillance camera systems, including those which use facial recognition algorithms as part of that system, and the use or processing of images or other information obtained by virtue of those systems. In the context of computer technology an 'algorithm' is simply a term used to describe a set of rules or processes to be followed when making calculations or problem solving.
- 1.2. The SCC is the statutory regulator of overt surveillance cameras which are used by the police in public places in England and Wales. His responsibilities include, in particular, regulating the use of surveillance cameras and their use in conjunction with LFR technology. It is the opinion of the SCC that when the police operate an overt surveillance camera system in public places their conduct amounts to being 'surveillance' which is conducted upon citizens by agents of the State. The SCC considers surveillance to be an intrusive investigatory power where it is conducted by the police which impacts upon those fundamental rights and freedoms of people, as set out by the European Convention of Human Rights (ECHR) and the Human Rights Act 1998. In the context of surveillance camera systems which make use of facial recognition technology, the extent of state intrusion in such matters is significantly increased by the capabilities of algorithms which are in essence, integral to the surveillance conduct seeking to harvest information, private information, metadata, data, personal data, intelligence and evidence. Each of the aforementioned are bound by laws and rules which ought to be separately and jointly considered and applied in a manner which is demonstrably lawful and ethical and engenders public trust and confidence.
- 1.3. Whenever the police seek to use technology in pursuit of a legitimate aim, the key question arises as to whether the degree of intrusion which is caused to the fundamental freedoms of citizens by the police surveillance conduct using surveillance algorithms (biometric or otherwise) is necessary in a democratic society when considered alongside the legality and proportionality of their endeavours and intent. The type of equipment/technology/modality which they choose to use to that end (e.g. LFR, ANPR, thermal imaging, gait analysis, movement sensors etc), the manner in which such technological means are deployed, (such as using static cameras at various locations, used with body worn cameras or other mobile means), and whether such technology is used overtly alongside or networked with other surveillance technologies, are all factors which may significantly influence the depth of intrusion caused by police conduct upon citizen's rights.

- 1.4. The provisions of this document only apply to the use of facial recognition technology and the inherent processing of images by the police where such use is integral to a surveillance camera system being operated in 'live time' or 'near real time' operational scenarios. This document is subordinate to, and should be read in conjunction with the SC Code. Its production does not effect changes to the SC Code in any way.
- 1.5. In the context of this guidance the operation in 'live time' of facial recognition algorithms refers to the deployment of surveillance camera systems by the police with the intention of conducting surveillance upon members of the public so as to capture their images which are then automatically processed in 'live time' so as to extract biometric data, specifically measurements of facial features, which is then immediately compared against biometric data contained on a watchlist which is held within a data base.
- 1.6. Also in this context, 'near real time' is a term which should be interpreted as being applicable to those circumstances whereby images are analysed by facial recognition technology very shortly (a matter of minutes) after the images are captured as part of a surveillance. It is acknowledged that 'near real time' is a relatively non-specific term which requires a degree of ethical interpretation to be applied by decision makers.

2. Biometrics, Equality and Ethics

Biometrics and LFR

- 2.1. The term ‘biometrics’ is described in the Home Office Biometrics Strategy (‘Better Public Services Maintaining Public Trust’) which was published in June 2018, as ‘the recognition of people based on measurement and analysis of their biological characteristics or behavioural data.’
- 2.2. In some respects facial biometrics have similarities to fingerprints as both can be captured without the need for any form of intimate sampling by the police and both involve parts of the body which are normally visible to the general public. Similarly, as with DNA, the use of facial recognition algorithms enables the extraction (albeit without the need for the use of force) of individually unique information, which is intrinsically private in character, enabling comparison and identification activity to be conducted by the police.
- 2.3. However, where LFR is distinctly different from other forms of biometrics, such as DNA and fingerprinting, is that it enables facial biometrics to be obtained without the knowledge or cooperation of the subject, or the use of force and on a mass scale. Unlike fingerprints/DNA the technological process of assessment of a facial biometric is not universal, for instance the facial template created by one proprietary system may not be portable between different systems provided by different suppliers and therefore may only have meaning in the particular system supplied and being operated.
- 2.4. In the context of the Data Protection Act 2018 (DPA) the use of LFR for the ‘law enforcement purposes’ constitutes ‘sensitive processing’ as it involves the processing of biometric data for the purpose of uniquely identifying an individual. Biometric data is defined for data protection purposes at Section 205(1) DPA. The Information Commissioner’s Office provides guidance regarding data protection legislation which they separately regulate.
- 2.5. The technical process associated with LFR in simple terms is broadly as follows:
 - a) The compilation of a database of images against which the biometric data of members of the public are to be compared (the watchlist).
 - b) Facial image acquisition by a surveillance camera in real time, of persons who pass within the view of the camera at a given location.
 - c) Detection by technology of human faces amongst images captured by the camera and the isolation of individual faces.
 - d) Feature extraction by the software resulting in a biometric template to that particular face.
 - e) Face comparison by the technology of the extracted features against those held within a watchlist.
 - f) The matching by the technology of extracted features with those held on a watchlist together with an indication of likeness generated by the software as a “similarity score” to be considered by a human, for a decision to be made thereafter.

- 2.6. System operators are able to set a “similarity threshold” on the system which informs the algorithms as to the extent of similarity between the two facial biometrics for which operators require a notification by the system. (See paragraph 4.66 – Similarity Threshold). Thereafter decisions are made by a human decision maker and police action (or inaction) takes place leading to an outcome.
- 2.7. The SCC considers that use of LFR is not analogous to the taking of photographs or the use of CCTV cameras by the police for the following reasons:
- a) LFR is a novel technology.
 - b) It involves the capturing of images and the near processing of digital/biometric information of a large number of members of the public in circumstances where the majority are of no interest to the police.
 - c) The information captured amounts to ‘sensitive’ personal data within the meaning of the Data Protection Act 2018, which represents an institutional recognition of the sensitivity of the data concerned which is not present in the case of ordinary photographs and images.
 - d) The sensitive personal data is processed in an automated way.
 - e) It may not be necessarily and wholly appropriate to equate the scanning of faces within a crowd by a police officer, whether visually or with still/video cameras, to the similar activity where it is conducted by the police when operating LFR to capture and compare the facial features of each individual in that crowd against a database. In the latter case, the ECHR intrusion is caused by means of a person’s biometric characteristics being indiscriminately scanned and then assessed by technology in the case of every individual which the technology sees, and in the view of the SCC requires a more detailed consideration of legal principles than in the case of more general police observation activities.

The Public Sector Equality Duty (PSED)

- 2.8. A statutory duty of the police whenever they are considering the use of LFR, is to comply, and to be able to demonstrate compliance, with their obligations arising from Section 149 of the Equality Act 2010, which are as follows:
- A public authority must, in the exercise of its functions, have due regard to the need to;
- a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act;
 - b) advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
 - c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.
- 2.9. The SCC recognises that technology advances rapidly and that the ‘training’ of algorithms to reduce inherent inconsistencies (or ‘bias’ as it is more commonly referred to) is delivering some positive outcomes in that regard. Many concerns have been expressed in the public domain in respect of the potential for facial recognition algorithms to produce results which are inconsistent, and thereby considered as discriminatory, depending upon the diversity of the demographics in which the

technology is operated. Such concerns largely arise from the potential for algorithms in some systems to be less accurate when producing an indication of likeness where faces are female, from members of the black, Asian and other ethnic minority communities in particular.

- 2.10. The SCC is aware that such matters attract scientific study and opinion, which indicates that the accuracy of a facial recognition system may be influenced by the data sets used to 'train' its capabilities. Specifically, that any imbalance as to the demographics of the system's training data sets may lead to a differential in the accuracy of the algorithms with respect to those demographics.
- 2.11. It is important for the police to recognise that the responsibilities which arise from the PSED do not just apply to the LFR technology, the cameras and the software. The responsibility applies to all aspects of the proposed conduct. By means of example; the LFR algorithms provide a qualified indication of similarity between images. However, the decisions of the 'human decision maker' determine whether a police intervention is justified and police action then follows. This decision making and operational activity takes place as part of the overall 'system' of operation. Therefore, the human decision making function is equally as relevant to the PSED duty which arises, as indeed is the wider spectrum of the organisational and operational approach. Though it may be considered as a contributing factor, the human decision maker is not in itself a sufficient fail safe to discharge the PSED responsibilities which arise, it is an ingredient of the overall approach which has to be considered and assessed as part of that duty (See paragraph 4.52 regarding human decision making).
- 2.12. The PSED is a duty of process and requires the taking of reasonable steps, assessed upon rigorous consideration of the context of the decision in question. It is an enduring responsibility which continues throughout the use of LFR and helps make the police more accountable, and their conduct more assuring to members of the public. Those statutory responsibilities include a requirement to take reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision or policy on people with the relevant characteristics.
- 2.13. The following established principles of the PSED are repeated below:
 - a) The PSED must be fulfilled before and at the time when a particular policy is being considered.
 - b) The duty must be exercised in substance, with rigour, and with an open mind. It is not a question of ticking boxes.
 - c) The duty is non-delegable.
 - d) The duty is a continuing one.
 - e) If the relevant material is not available, there will be a duty to acquire it and this will frequently mean that some further consultation with appropriate groups is required.
 - f) Provided the court is satisfied that there has been a rigorous consideration of the duty, so that there is a proper appreciation of the potential impact of the decision on equality objectives and the desirability of promoting them, then it is for the decision-maker to decide how much weight should be given to the various factors informing the decision.

- 2.14. It is important therefore that those making decisions relating to the procurement, deployment and operation of facial recognition technology, take all reasonable steps to satisfy themselves either directly or by independent verification, as to the question as to whether the software to be procured and operated in public presents inherent risk of inconsistency in its ability to recognise and assess a diversity of facial features. The police should take reasonable steps to establish whether a risk of inconsistency exists in the performance of the software or their wider operational conduct in connection with which the software is to be used. Where any such risk is identified, such risks should be assessed and considered in the context of risk mitigation measures so as to determine whether they may be satisfactorily removed or mitigated. This responsibility endures throughout their intended conduct. It may be that in some cases appropriate access rights may require negotiation with suppliers so as to enable a police force to be able to audit the necessary technical detail. That is a matter for the procuring Chief Officer and Police and Crime Commissioner.
- 2.15. Any unreasonable restrictions to police scrutiny which are made by or on behalf of a supplier, for example unreasonably asserting intellectual property rights etc. as a suggested bar to enabling appropriate police enquiry being made, should be a factor of the PSED assessment process and not necessarily be considered in themselves as being a reasonable excuse for an appropriate degree of scrutiny not being undertaken. If, having taken all reasonable steps to understand any risks of inconsistency which occurs within the software, such risks continue to exist, then the police should be able to justify how their policies, decision making and conduct takes account of such risks and how they are to be satisfactorily mitigated. Where this is the case, the SCC recommends that guidance is sought by the police from their legal advisers as to the proper discharge of their PSED responsibilities before any use of the LFR software takes place. If the technology cannot be deployed in a manner whereby the PSED has not or cannot be discharged then it should not be used.
- 2.16. The SCC considers that meaningful engagement and consultation with communities, and the collation, analysis and publication of relevant data are important considerations which are integral to the PSED. (See Section 6, Public Engagement, Provision of Information, Performance).
- 2.17. **The SCC recommends that the Home Office consult with others including the National Police Chief's Council and the Association of Police and Crime Commissioners to establish;**
- a) **a national procurement strategy which provides the right tools and engenders public confidence;**
 - b) **a means by which the credentials of LFR technology can be suitably analysed and assessed so as to determine risks associated with matters such as accuracy, similarity thresholds, human decision making (amongst others);**
 - c) **national standards (e.g. privacy/security by design/default) to help to inform future procurement, equipment employment and deployment decision making as well as better enabling the police to comply with the Public Sector Equality Duty (PSED) and other statutory and risk assessment obligations in respect of their use of LFR.**

Ethics

- 2.18. In the context of policing, the systems of moral values and professional standards which drive and influence police activity in a manner which is transparent are fundamental to public trust and confidence. In the context of LFR acting lawfully and acting ethically are separate but inextricably linked considerations. A relevant and helpful mantra to consider from the NSCS is; “Just because you can” doesn’t mean “you should”.
- 2.19. Those police forces intending to use LFR technology may also wish to consider engaging with the National Police Chief’s Council (NPCC) appointed lead for Ethics in respect of their planning, operational and post event activities. The SCC supports as being good practice, that any use of LFR by the police is notified to the NPCC Information Management and Operational Requirements Coordinating Committee (IMORCC) before any such conduct takes place.
- 2.20. Although not a feature of the SC Code, a series of high-level principles have been developed by the Biometrics and Forensics Ethics Group for consideration of the ethical issues to be addressed in relation to the operation of biometric and forensic capabilities. Those ethical principles should be demonstrably applied by the police whenever operating LFR. They are as follows:
- Procedures should be used to enhance public safety and the public good;
 - Procedures should be used to advance justice;
 - Procedures should respect the human rights of individuals and groups;
 - Procedures should respect the dignity of all individuals;
 - Procedures should, as far as possible, protect the right to respect for private and family life where this does not conflict with the legitimate aims of the criminal justice system to protect the public from harm;
 - Scientific and technological developments should be harnessed to promote the swift exoneration of the innocent, afford protection and resolution for victims and assist the criminal justice process;
 - Procedures should be based on robust evidence.
- 2.21. The details as to the relevant Ethical Principles are accessible at the attached link:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702184/Biometrics_and_Forensics_Ethics_Group_principles_website_v2.pdf

- 2.22. Similarly applicable is the commendable ‘Code of Ethics’ which has been produced by the College of Policing. The aim of the Code of Ethics is to support each member of the policing profession to deliver the highest professional standards in their service to the public. The Code of Ethics issued by the College of Policing is accessible via the following link:

https://www.college.police.uk/What-we-do/Ethics/Ethics-home/Documents/Code_of_Ethics.pdf

2.23. The Centre for Data Ethics and Innovation (CDEI) is an independent expert committee, led by a board of specialists, set up and tasked by the UK Government to investigate and advise on how we maximise the benefits of AI and data-driven technology. Their goal is to;

“create the conditions in which ethical innovation can thrive: an environment in which the public are confident their values are reflected in the way data-driven technology is developed and deployed; where we can trust that decisions informed by algorithms are fair; and where risks posed by innovation are identified and addressed.”

- 2.24. Specifically, with regards to the use of LFR in law enforcement, the CDEI expects police forces to be appropriately transparent about how they use this technology, including where it is deployed, the basis by which people are included on watchlists, and how deployments are signed off. The CDEI support calls for greater consistency in how LFR is used by different forces, including having minimum safeguards in place before each rollout is confirmed.
- 2.25. In the interests of greater transparency and integrity, the SCC recommends as good practice the establishment of procedures whereby decision making by the senior officers which approve the procurement and overt deployment of LFR is made available for scrutiny by the local Ethics Committee structures, with due regard given to matters of confidentiality as appropriate.
- 2.26. **The SCC recommends that where police forces are considering operating LFR they should develop mechanisms which provide for meaningful and independent ‘ethical oversight’ of their decision making and operational conduct. Such considerations should be applied as part of the initial police planning processes and be established before any operational activity commences. Ethics Committees, where they exist, may meaningfully be consulted in the first instance and any relevant oversight arrangements determined. Where there is no digital or ethics committee structure within a police force region there may be local multi agency structures which could play such a role, similar to those which exist in scrutinising police stop and search activities for example. Such matters are for Chief Officers and their Police and Crime Commissioners to consider where relevant. The SCC is supportive in particular of including the police use of LFR within the ambit of decision making which should be covered under the establishment of a national Digital and Data Ethics Committee by APCC and NPCC.**

3. Human Rights, ‘In Accordance with the Law’ and The Legal Framework

Human Rights

- 3.1. The Human Rights Act 1998 enshrines the fundamental rights, freedoms and protections that citizens within the UK are entitled to from intrusion by the State as provided by the European Convention on Human Rights. According to Convention case law, any interference with a person’s right to a private life must satisfy the following test:
- a) there is a legitimate public interest as set down in Article 8(2) (namely in the interests of national security, public safety or the economic wellbeing 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);
 - b) the limitations on the right are “in accordance with the law” or “prescribed by law” (lawful); and,
 - c) the limitations are “necessary in a democratic society” for the purpose of protecting one of the legitimate interests (proportionality test). A limitation will be necessary in a democratic society if it answers to a “pressing social need”, that is, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are “relevant and sufficient”. “Necessary” in this context does not have the flexibility of such expressions as “useful”, “reasonable”, or “desirable”.
- 3.2. In the context of the overt operation of surveillance camera systems in public places, Article 8 (respect for private and family life) is a key consideration for system operators to address, but is by no means the only Convention right which is engaged. There is also potential impact on other article rights including (but not restricted to):
- the right to freedom of assembly
 - freedom of thought, belief and religion
 - freedom of expression
 - freedom of association
 - the protection from discrimination in respect of those rights and freedoms
- 3.3. An assessment of potential harm and impact upon those rights and freedoms is an essential consideration to be made by the police, as part of each and every intended deployment of LFR, and before any such deployment of the technology is made. An assessment of risk, including an assessment of intended and collateral intrusion, together with the identification and implementation of risk management measures, should be conducted and documented as part of police policy. The creation of publicly accessible policies which set out the safeguards to be applied to police discretion is a necessary ingredient for such conduct to be considered as being ‘in accordance with the law.’ (See paragraph 3.5). The SCC considers that it is important to make a distinction between a Data Protection Impact Assessment (DPIA) together with the associated policy document requirements which arise from DPA 2018, and those risk

assessment and policy considerations which address the wider statutory, operational and organisational responsibilities applicable to the use of LFR which go beyond the protection of personal data.

- 3.4. Depending upon the manner in which it is to be operated in any given situation, the overt use of LFR by the police may fall within the common law powers of the police to obtain information for policing purposes and the compilation of watchlists may be authorised by the Police and Criminal Evidence Act 1984 and to some extent the common law. Those are matters which the police ought to consider when intending to operate LFR where determining their justification for acting ‘in accordance with the law’ and on a case by case basis, in consultation with their legal advisers as necessary.

In Accordance with the Law

- 3.5. The general principles which are applicable to the question as to whether the police conduct using LFR is ‘in accordance with the law’ are reproduced below. Those principles are important where the police are considering establishing and implementing policies which set out the safeguards which are to apply in limiting their discretion when deciding who they will be placing on a watchlist and where and when their conduct is to take place. (See paragraphs 3.34 to 3.58)
- a) “The measure in question, must have some basis in domestic law, and must be compatible with the ‘rule of law’ which means that it must comply with the two requirements of ‘accessibility’ and ‘foreseeability’.
 - b) The legal basis must be ‘accessible’ to the person concerned, meaning that it must be published and comprehensible, and it must be possible to discover what its provisions are. The measure must also be ‘foreseeable’ meaning that it must be possible for a person to foresee its consequences for them and it should not ‘confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself’.
 - c) Related to (b), the law must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.
 - d) Where the impugned measure is a discretionary power, (a) what is not required is ‘an over-rigid regime which does not contain the flexibility which is needed to avoid an unjustified interference with a fundamental right’ and (b) **what is required is that ‘safeguards should be present in order to guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights’** (bold for additional emphasis), (per Lord Hughes in *Beghal v Director of Public Prosecutions* [2016] AC 88 at [31] and [32]). Any exercise of power that is unrestrained by law is not ‘in accordance with the law’.
 - e) The rules governing the scope and application of measures need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them.
 - f) The requirement for reasonable predictability does not mean that the law has to codify answers to every possible issue.”
- 3.6. The legal framework which is applicable to the overt use of LFR is set out in the following paragraphs.

The Legal Framework

- 3.7. In the context of the sufficiency of the current legal framework to accommodate police conduct using LFR; where the police are seeking to determine the ‘legality’ of their overt use of LFR, it is “crucial” to those deliberations, and on a case by case basis, that they are clear as to whether or not the LFR system of operation is such that the data of anyone captured by the software is automatically and almost instantaneously deleted without any human observation being applied where there is no match with a person on a watchlist. The police should be transparent and suitably explicit as to the legal basis upon which they seek to rely in order to justify their conduct and should address this particular point as part of their considerations when establishing policies. The legal framework which underpins the overt use of LFR in public places where the above does apply is as follows:
- The Common Law
 - The Data Protection Act 2018
 - The Protection of Freedoms Act 2012
 - The Surveillance Camera Code of Practice
 - The detailed policy documents of those police forces conducting surveillance using LFR technology.
- 3.8. Depending upon how LFR is to be used in any given circumstances, the above framework may provide a degree of certainty and foreseeability as to the clear legal standards against which the conduct of the police is to be held. In particular, the content of police policies which set out the safeguards which are to be applied to guard against overbroad police discretion where deciding who is to be placed upon a watchlist and where the technology may be used are important considerations in that regard. (See paragraphs 3.34 to 3.58).
- 3.9. There are of course broader statutory considerations which may apply to aspects of the intended police conduct when operating LFR overtly, such as the Regulation of Investigatory Powers Act 2000 (RIPA) specifically where an overt surveillance camera system is used to conduct covert surveillance. (See paragraphs 3.59 to 3.74 below). Also, the Criminal Procedure and Investigations Act 1996 (CPIA) applies where material derived from police conduct is to be used and considered for disclosure purposes as evidence in judicial proceedings. (See paragraphs 5.6 to 5.11 below).
- 3.10. A brief explanation as to the applicability of each element of the relevant legal framework is as follows;

The Common Law

- 3.11. The common law is simply the body of law declared by judges and derived from custom and precedent. The common law powers of the police to obtain and store information for a policing purpose may in some circumstances be applicable to the police use of LFR and compilation of the watchlist. The SCC urges police forces to seek legal guidance on these matters in connection with their intended conduct, before any such conduct commences.

The Data Protection Act 2018

- 3.12. The Information Commissioner regulates the Data Protection Act 2018 (DPA). The Act is the UK's implementation of the GDPR and provides statutory responsibilities which extend to operators and users of surveillance camera systems alike in respect of the processing and use of personal data obtained by virtue of the use of those systems. The 'Guiding Principles' within the SC Code signpost the data protection considerations which apply when overtly operating surveillance camera systems in public places in England and Wales. (See Appendix B for the Guiding Principles of the SC Code). The regulatory guidance of the Information Commissioner's Office should be sought in all matters relevant to the DPA 2018 where necessary.
- 3.13. The legal protections provided by the DPA are an important part of the legal framework which may underpin the police use of LFR. It enables the proportionality of interference with Article 8 (privacy) to be adequately examined in the context of processing personal data, which amounts to being "sensitive processing," it enables an examination to be conducted as to the question whether there was a proper "law enforcement purpose" applicable to the data processing attributable to the use of LFR and whether the use of LFR was "strictly necessary" in that regard.
- 3.14. The provisions of the DPA provide statutory responsibilities for the Data Protection Officer (DPO) and a Data Controller. The SCC recommends that it is good practice for the Senior Responsible Officer, who is designated by the Chief Officer as having overall responsibility for strategic oversight for the police conduct using LFR (see paragraph 4.4), to ensure effective coordination between the senior police decision makers, operational commanders, exhibits officers, disclosure officers, Authorising Officers (RIPA where relevant) the Data Controller and DPO with regards to that conduct. In doing so the statutory requirements of the DPA may be better considered and accommodated alongside other statutory and procedural responsibilities which apply to the police conduct, for example those relevant to the integrity, management and continuity of evidence, the management of risk and the duty of care obligations which arise. (See Section 4 regarding "Governance").
- 3.15. In the context of LFR where the processing of data is "sensitive processing" then such processing must be strictly necessary for the law enforcement purposes, the processing must meet at least one of the conditions in Schedule 8 DPA and at the time when the processing is carried out the Data Controller must have an appropriate policy document in place in accordance with Section 42. A Data Controller is required to document policy, and risks associated with Article 8 as part of a DPIA as required by Sections 64(3)(b) and (c). The requirements as to what a policy document should contain are set out at Section 42 and includes:
- an explanation of how the processing complies with the relevant data protection principles;
 - an explanation of the controller's policies in relation to retention and erasure of personal data, including an indication of how long the data is likely to be retained.

- 3.16. **The law enforcement purposes**, are described at Section 31 DPA as follows:
‘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.’
- 3.17. Schedule 8 sets out conditions for sensitive processing under Part 3 and provides that the condition in paragraph 1 is met if the processing a) is necessary for the exercise of a function conferred on a person by an enactment or rule of law, and b) is necessary for reasons of substantial public interest.
- 3.18. Additionally, the statutory provisions include a requirement to complete a data protection impact assessment (DPIA). The SCC has developed a DPIA template in conjunction with the ICO specifically for organisations in England and Wales that must have regard to the SC Code by virtue of Section 33(1) PoFA. The DPIA process enables a Data Controller to assess whether the use of surveillance camera technologies meets a stated purpose in a way which is proportionate to the level of privacy intrusion caused by its use. The template is available on the SCC website which may be accessed via the below link. It may not be suitable for the use of assistive technology which is being considered. Guidance issued by the ICO should be considered in respect of such matters.

<https://www.gov.uk/government/publications/privacy-impact-assessments-for-surveillance-cameras>

- 3.19. The ICO has issued its own, non-statutory code of practice document; ‘In the picture: A data protection code of practice for surveillance cameras and personal information’ which can be accessed by the following link:

<https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

The Protection of Freedoms Act 2012 (PoFA)

- 3.20. Chief Officers of Police and Police and Crime Commissioners in England and Wales are “relevant authorities” as defined by Section 33(5) PoFA and as such are subject to a statutory duty to have regard to the SC Code when operating surveillance camera systems in public places (s33(1)). For completeness Section 33 of PoFA provides the following:

“(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 of 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.”

- 3.21. In consideration of Sections 33(3) and 33(4) above, any failure by a relevant authority to have regard to the SC Code in respect of images or other evidence derived from a surveillance camera system to which PoFA applies, should be disclosed to the Crown Prosecution Service (CPS) whenever such images or other evidence as to the operation of that system is to be adduced in to judicial proceedings. The duty of disclosure enables the CPS to properly apply a disclosure test in accordance with the provision of the Criminal Procedure and Investigations Act 1996. (See paragraphs 5.6 to 5.13 regarding “Evidence”).
- 3.22. Section 29(6) describes surveillance camera systems to which the Act and the SC Code applies as follows:

‘(6) In this Chapter “surveillance camera systems” means;

- (a) closed circuit television or automatic number plate recognition systems,
- (b) any other systems for recording or viewing visual images for surveillance purposes,
- (c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or
- (d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).’

- 3.23. The use of facial recognition technology and indeed any other technology which is integrated with the use of a surveillance camera system as defined above, is therefore capable of falling within the aforementioned statutory definition and thereby the provisions of PoFA and the SC Code.

The Surveillance Camera Code of Practice

- 3.24. The SC Code is issued by the Secretary of State by virtue of Section 30 of PoFA and provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities, including the police, and other system operators who voluntarily adopt its provisions. The SC Code is accessible by the following link:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

- 3.25. The SC Code contains a number of provisions which are of specific relevance to the use of facial recognition and other technologies integrated with the operation of surveillance camera systems. In particular those provisions include the following comment:

‘The Surveillance Camera Commissioner will be a source of advice on validation of such systems’ (Foot note 4).

- 3.26. In this context, the SCC advises that the term ‘validation’ means that a system is **demonstrably** being operated in a manner which has **regard** to the SC Code and such **regard** is supported by an appropriate audit trail. In particular an audit trail should include endorsement in the police policy documents that the surveillance camera system being used to which LFR is integral, is to be operated in accordance with Section 33(1) PoFA and in a manner which is consistent with the provisions of the SC Code. There should also be a completed “Self-Assessment Tool” (SAT) which demonstrates the nature of compliance in that regard (see paragraph 3.28 below). The validation of any application of a facial recognition system should follow the risk-based approach laid down in the Forensic Science Regulator’s Codes of Practice and Conduct and that this should be carried out prior to any live deployment of a new system taking place.
- 3.27. The risk assessment element of this framework is an important way of ensuring that the validation study is scaled appropriately to the needs of the end-user, which in the case of law enforcement use, would normally be the Criminal Justice System as a whole rather than any particular analyst or police force. (See also paragraph 4.77 – Operational Trials).
- 3.28. The SCC seeks to discharge his particular responsibilities with regard to “validation” by a number of means which importantly, require early engagement by the relevant police force with the SCC offices. The responsibility for early engagement with the SCC lies with the Chief Officer of the force concerned. The SCC will consider the Self-Assessment Tool which should be completed in sufficient detail by the relevant police force and forwarded to the offices of the SCC so that it is received by the regulator at least five working days before operational activity is commenced. Thereafter the SCC will consider what further matters require consideration before determining the validity of the operation of the LFR system as being conducted in accordance with the SC Code so as to satisfy the provisions of Section 33(1) PoFA. The Self-Assessment Tool is available on the SCC website and accessible via the following link:
- <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool>
- 3.29. The duty placed upon the police by virtue of Section 33(1) PoFA to have regard to the SC Code arises from the importance which Government places on the operation of surveillance cameras in public spaces, being undertaken to a standard in which the public can derive trust and confidence in the legitimacy and integrity of their use.
- 3.30. Completion of a Self-Assessment Tool (SAT) demonstrates a detailed and transparent approach to compliance with the SC Code, together with the requisite internal governance arrangements which are in place, together with an appropriate audit trail as to such issues. The completion of a SAT is not a statutory requirement. Allocation of individual responsibility for completing and maintaining a review of the SAT is for police decision makers to determine.
- 3.31. A further benefit of a completed SAT is that it enables an assessment to be conducted by a police decision maker as to the extent to which the intended operation of a surveillance camera system accords with the guiding principles of the SC Code. It also highlights areas which require further action to address any shortfall in compliance. However, where a relevant authority does not complete a SAT in respect of an LFR

surveillance camera system it should otherwise ensure that it has an audit trail which enables it to sufficiently demonstrate compliance with Section 33(1) PoFA and the SC Code. Furthermore, ‘Guiding Principle 10’ of the SC Code (paragraph 4.10.1) requires that regular reviews should be carried out of the use of a system so as to ensure that its use remains necessary, proportionate and effective in meeting its stated purpose for deployment. The SAT may be used to assist with such a review.

- 3.32. The frequency by which a SAT is completed and/or updated by a relevant authority is dependent upon the circumstances in connection with which the surveillance camera system is operated and on a case by case basis. Each case must be assessed on its particular merits. In the context of LFR, the SCC considers that such systems are in general, more likely to be operated lawfully and legitimately where they are so operated for a defined period of time in support of clearly stated operational objectives, rather than in circumstances whereby they are operated for more generic monitoring purposes in a manner which is similar to that provided by fixed CCTV systems. LFR should not be deployed any longer than necessary to meet its intended purpose. In determining when to refresh a SAT, the key test is whether the SAT continues to appropriately and accurately reflect the proportionality, nature of purpose and the manner in which the technology is being used, the inherent risks and addresses the key principles within the SC Code. If not, or the circumstances or risks associated with such operation change, then a new SAT should be considered and the legitimacy of continuing police conduct re-assessed by the senior police decision maker. (See paragraph 4.6 regarding “Approval”).
- 3.33. As a matter of transparency and good practice, it is recommended that a SAT is published so as to be accessible to members of the public. (See paragraphs 3.84 – 3.91 below regarding risk assessments).

Police Policy Documents – Legitimacy and Specificity (The 5WH)

- 3.34. It is established case law that local (police) policies can be relevant to considerations which satisfy the requirement of the conduct of the police being considered to be “in accordance with the law”. Such policies do not necessarily have to be at a national level. The policies produced by the police as part of their conduct using LFR can be a key ingredient of the legal framework regarding the use of the technology and should be produced in such a manner so as to include the necessary safeguards which govern all aspects of police discretion and decision making which may impact upon ECHR rights, particularly with regards the question of who is to be placed upon a watchlist and where the technology is to be used. Those policies where they are produced should be cognisant of the principles illustrated at paragraph 3.5 above.
- 3.35. The SC Code (paragraph 4.12.2 SC Code) requires system operators to have ‘a clear policy to determine the inclusion of ... a known individual’s details on the reference database associated with such technology.’ In the context of the policies produced by the police arising from their LFR activities, it is important that those policies are of sufficient detail particularly in respect of the matters set out in this guidance at paragraphs 3.38 to 3.58. They do not need to codify every possible scenario which may arise; however, they should lay down principles which are capable of being predictably applied to any situation. In particular it is important that police policies are sufficiently **specific** as to the safeguards which are in place to constrain the actions and

discretion of the police and how those safeguards will be applied. It is recognised that the legitimate interests of law enforcement and national security may require a degree of confidentiality in delivering effective lawful conduct the nature of which is for police decision makers to determine. (See paragraph 6.7).

- 3.36. A fundamental principle which underpins the use of any overt surveillance camera system is that its use must be in pursuit of a legitimate purpose to meet an identified pressing need. (Guiding Principle 1 of the SC Code). Those issues should be clearly set out in the policies which the police produce.
- 3.37. In particular, clarity should be provided as to the parameters of the police conduct which is to be undertaken when using LFR, commonly referred to by the SCC as being the '5WH' question, (What, Who, Why, Where, When and How), together with the requisite safeguards which regulate police discretion on such matters. Decisions which are made in respect of each of these considerations should be made on reasonable grounds which in themselves are grounded in information and facts and are not speculative. Those considerations which are specific to each of the '5WH' may overlap to varying degrees depending upon the relevant circumstances in which LFR is to be operated. The decisions made and the safeguards applied should be recorded and be capable of independent scrutiny. The SCC recommends that the following specifics are addressed by decision makers:
 - 3.38. **WHAT** – What is the problem to be investigated or otherwise addressed by police action and what is sought to be achieved by the intended conduct?
 - 3.39. In the first instance, it is important that the police specifically define the pressing problem which they seek to address and the case for compulsion for them to act. In so doing, judgement can be better exercised as to the legitimacy of any proposed action to address that problem. Having defined the specific problem, a clear case of justification for use of LFR should be set out, which is based upon information and facts. Whilst it may not always be necessary for there to be evaluated intelligence logs which provenance a particular pressing need, it would in the interests of greater transparency for there to be an audit trail which accurately illustrates the existence, nature and extent of the problem which the police are seeking to address and which includes an indication as to the provenance/accuracy of the information provided (with due regard applied to the need to protect sensitive matters of confidentiality).
 - 3.40. **WHO** – Who are the individuals to which the police conduct using LFR, is to be directed? How are those individuals selected for inclusion on a watchlist and what are the safeguards relevant to decision making?
 - 3.41. Refer to the 'Watchlist' section commencing at paragraph 4.20.
 - 3.42. **WHY** – Why is it considered to be necessary and proportionate to conduct surveillance by means of a surveillance camera system enhanced with LFR technology against known individuals in the context of what the police seek to achieve?

- 3.43. It is important for the police to justify in clear terms, and on reasonable grounds, why they are intending to address an identified problem or pressing need by means of the deployment of LFR against particular subjects in an area, rather than use other tactics. Specifically, there should be clear rationale recorded as to what the strategic and tactical aims and objectives are and why LFR is considered to be necessary and proportionate to achieve those aims. Further guidance is provided at paragraphs 3.75 (Necessity) and 3.78 (Proportionality).
- 3.44. **WHEN** – When is it intended to operate LFR in terms of times/days of the week etc. and what is the duration/lifespan of the intended operational conduct?
- 3.45. Determining the ‘WHAT’, ‘WHO’ and ‘WHY’ questions will assist decision making as to the ‘WHERE’, ‘WHEN’ and ‘HOW’ questions and the attendant specifics of police safeguards/policies which may be relevant.
- 3.46. In general (though exceptions may exist arising from the nature of the problem to be addressed by means of LFR and inherent risks which arise) it may be less justifiable to deploy LFR at particular locations to search for individuals, simply on the basis that a large volume of people frequent or pass through the area and it is hoped that a person on a watchlist may be amongst the crowds. Rather, the police should be able to demonstrate that decisions as to when and where they look for persons who they seek by means of LFR, are based upon reasonable grounds. Those reasons should be recorded and be capable of being objectively and independently considered.
- 3.47. The SCC recommends that operations which make use of LFR should be “timebound” in that the police surveillance conduct using the technology should have clear start and end times and dates, together with a timetable established for regular reviews which are to be conducted by police decision makers. (See paragraph 4.6).
- 3.48. Care should be exercised when considering the timings of operations for instance where they may clash with religious festivals or anniversaries of incidents which may cause heightened community tension etc. or where there is poor light or other physical characteristics of the intended location(s) which may impact upon accuracy of the technology.
- 3.49. Policies should also set out the arrangements for keeping the timings and duration of activity to the minimum necessary to achieve its objectives or otherwise assess that the objectives cannot or are unlikely to be achieved to the extent that police conduct may no longer be justified. Where conduct is not lawfully justified it should not take place.
- 3.50. **WHERE** – Where is it intended that the police conduct using LFR will take place?
- 3.51. Decisions regarding the location and timings of the deployment of LFR should be based upon reasonable grounds that the persons on a watchlist who they seek to locate, or that the problem which they seek to address necessitates the deployment of LFR at a particular location at particular times.
- 3.52. In determining the location at which LFR is to be deployed, appropriate consideration should be made as to the impact upon the fundamental rights and freedoms of people within that location, regardless as to whether they are on the relevant police watchlist. In particular members of the public may be discouraged or inhibited from otherwise

exercising their legitimate rights in the vicinity of where the LFR cameras are located, (usually referred to as the “chilling effect”). For example, citizen’s rights such as the right of privacy, freedom of religion, freedom of expression, freedom of assembly may be inhibited for example where LFR is deployed proximate to places of religious worship, at schools where children or parents gather or at lawful protests. There may be additional considerations which apply where deployments are considered in areas where there are vulnerable communities or community tensions are high.

- 3.53. Police policies ought to set out the safeguards attributable to limiting police discretion as to the location and timings of LFR deployments. It is also important to note that the SC Code (paragraph 3.3.6 SC Code) provides the following “This is not to imply that the exact location of surveillance cameras should always be disclosed if to do so would be contrary to the interests of law enforcement or national security.”
- 3.54. **HOW** – How is it intended to conduct the use of LFR in the circumstances described and how will risk be managed?
- 3.55. The nature of the LFR technology and method by which it is to be deployed and operated should be addressed in police policies. There should also be an explanation provided as to how the public are to be made aware that surveillance by means of LFR is taking place, how human intervention in decision making will be facilitated and what police action is proposed. (See Section 6). The nature and intensity of the proposed surveillance activity should also be considered and determined, whether it be the volume of cameras used or the means or regularity/frequency by which they are deployed (for example mounted on marked police vans, or integrated within the CCTV system of a third-party private operator of an LFR system). Such considerations extend to whether systems owned or operated by third party operators/organisations, are to be used as an ingredient of the police surveillance capability. (See paragraph 4.70 – Partnerships).
- 3.56. The SCC recommends that it is good practice for the police to consider having arrangements in place which ensures that the operational conduct of LFR in a public place, and the specific parameters of the operational conduct, are clearly set out and approved by a police officer of appropriate seniority in the organisation who is not engaged in the day to day direction of the operational conduct, similar in nature to that which exists within RIPA. Those who conduct activity within the terms of an operation should be aware of the extent to which such activity is approved. A suggested model of governance and decision making is offered by the SCC by which police conduct using LFR may be considered and approved as necessary, by police decision makers. (See paragraphs 4.6 to 4.19).
- 3.57. The application of legal principles which govern overt surveillance to particular facts is ultimately a matter of judgment for those police decision makers who grant approval for such activity to be conducted. Each case should be considered on its particular merits.
- 3.58. Having considered the “in accordance with the law” question, the applicable “legal framework” and the “specificity (5WH)” details set out above, those who are considering approving the police operational conduct utilising LFR should also decide whether such conduct amounts to being surveillance which is overt or covert in nature and whether such conduct is necessary in the circumstances (paragraph 3.75) and proportionate (paragraph 3.78) to what is sought to be achieved.

The Regulation of Investigatory Powers Act 2000 and Overt Surveillance Camera Systems

- 3.59. The “Home Office Revised Code of Practice (CoP) for Covert Surveillance and Property Interference” issued pursuant to Section 71(4) Regulation of Investigatory Powers Act 2000 (RIPA) explains that **overt** surveillance camera systems are capable of being used to conduct **covert surveillance** to the extent that an authorisation may be required under the provisions of that particular legislation (paragraph 3.39 RIPA CoP refers and is reproduced in the below section at paragraph 3.68).
- 3.60. The deployment of LFR enhanced surveillance camera systems by the police to look at and capture images of people, is conduct which amounts to being “surveillance” of citizens as it involves the monitoring and observing of persons. Surveillance is not a term which is defined within PoFA or the SC Code, albeit that a “surveillance camera system” is so defined at Section 29(6).
- 3.61. The use of overt surveillance cameras by the police using LFR does not normally require an authorisation under the Regulation of Investigatory Powers Act 2000 (RIPA). Members of the public should be made aware that such overt systems are in use for example, by virtue of the cameras or signage being clearly visible, through the provision of information and by undertaking consultation activities etc. (Paragraphs 6.1 to 6.7 refer).
- 3.62. It is important that those making decisions regarding LFR, and those engaged in the police conduct which uses it, understand the relevant provisions of RIPA so as to identify any risk of the police overt surveillance conduct using LFR becoming covert surveillance due to the manner in which the system is being operated. Being so aware will reduce the risk of covert surveillance being conducted outside of the provisions of the relevant legislation and ensure that the guidance of an Authorising Officer (RIPA) is sought in appropriate circumstances.
- 3.63. **Surveillance** – Surveillance is defined at Section 48(2) of the Regulation of Investigatory Powers Act 2000 in the context of covert surveillance as follows;

“surveillance” includes (a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; (b) recording anything monitored, observed or listened to in the course of surveillance; and (c) surveillance by or with the assistance of a surveillance device.’

- 3.64. **Covert Surveillance** – Section 26(9)(a) RIPA describes **covert** surveillance as follows:

“Surveillance is covert if and only if it is carried out in a manner that is calculated to ensure that the persons who are subject to the surveillance are unaware that it is or may be taking place.”

3.65. **Overt Surveillance** – The SC Code explains at paragraph 1.1 that;

“**overt** surveillance means any use of surveillance for which authority does not fall under the 2000 Act (RIPA)”

3.66. Paragraph 4.12.3 SC Code is clear however that;

“There may be occasions when the inclusion of information about an individual in a reference database with the intention of undertaking surveillance can be considered as covert surveillance and thus fall with the bounds of the 2000 Act.” (RIPA).

3.67. When considering these matters, it is important that decision makers recognise the distinction between the overt/covert nature of the **surveillance camera system** being operated, and the overt/covert nature of the **surveillance activity** being conducted by the police by means of it.

3.68. The Home Office Code of Practice for Covert Surveillance and Property Interference (RIPA) explains the following at paragraph 3.39.

“...where **overt** (bold for emphasis) CCTV, ANPR or other **overt** surveillance cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV, ANPR or other overt surveillance cameras in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

Example: A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual, such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual’s movements should be considered for authorisation as directed surveillance.”

3.69. The information which is sought or gathered about a subject by the LFR system, whether in itself or when assessed alongside other information held by the police, may amount to being “private information” as described at Section 26(10) RIPA.

- 3.70. Particular care should be taken where the purpose of targeting an individual using LFR is to gather information about them in circumstances where there is no foreseeable operational requirement for the police to stop and talk to that individual once they have been located by the LFR system. In such circumstances it is less likely that the subject will be aware that they are, or have been the subject of surveillance by the police. Any actions of officers which are deliberately undertaken so as to ensure that a person is unaware that police surveillance activity using LFR as part of a pre-planned operation is or may be taking place, may render the surveillance conduct as amounting to being covert in nature, whether in whole or in part and therefore that conduct may require of an authorisation under RIPA. (See paragraphs 4.45 to 4.50).
- 3.71. That is not to say that those persons who are targeted by the police using LFR for intelligence gathering purposes are subject to covert surveillance in every case, it is simply illustrative that such possibility exists and requires due consideration.
- 3.72. The decisions made in this context and the supporting rationale should be recorded and addressed in appropriate policies, with due regard given to matters of confidentiality.
- 3.73. Each police force has a “Covert Authorities Bureau” (CAB) or similarly named department which maintains a “Central Register of Authorisations” as required under the terms of RIPA. The SCC recommends as being good practice that the circumstances of proposed deployments of LFR by the police, together with the construct of the LFR watchlist are discussed with the local Covert Authorities Bureau (CAB) and considered by a force Authorising Officer (RIPA) before any operational activity is conducted, so as to determine whether an authorisation is required for the intended surveillance activity in accordance with the provisions of RIPA. Doing so will also help to ensure that the creation of a watchlist, the intended overt operation or any other factor of the operational intent does not give rise to risks associated with the conduct being outside of the law (e.g. RIPA), enable a better assessment to be made as to any risks to a source of, or use of, an image and also help to avoid any risk of conflict or compromise with any other operational activity being conducted by the relevant police force (a “blue on blue” risk).
- 3.74. RIPA and the attendant Codes of Practice are regulated by the Investigatory Powers Commissioner’s Office. Advice and guidance may be sought in respect of these matters from the police CAB, Authorising Officer (RIPA) or from the IPCO where necessary.

Necessity

- 3.75. Importantly, to comply with human rights law and to demonstrate that policy formulation encompasses human rights considerations, the police conduct must be “necessary in a democratic society.” It is therefore for the police to ensure that they have relevant and sufficient reason for any ECHR interference caused by their LFR conduct and that these are convincingly established and transparently set out. In the context of PoFA it is a requirement of the SC Code that surveillance camera systems being operated in public places must always have a clearly defined purpose in pursuit of a legitimate aim and be **necessary** to address a pressing need.

- 3.76. It is recommended (as set out at paragraph 3.39 above) that the problem which is to be addressed by the police by means of the use of LFR can be demonstrated by means of an audit trail, and that the grounds upon which it is believed that the operational conduct and use of LFR, is necessary are set out. The grounds of necessity may for example be the prevention and detection of crime, public safety, national security etc. It is important that the police set out why their proposed **operational conduct** is considered necessary rather than simply desirable, convenient, or is otherwise borne out of no other reason than having the technical capability at their disposal.
- 3.77. In the context of sensitive processing of personal data, the DPA (Section 35(5)(a)) additionally requires that, where sensitive processing without the consent of the data subject is conducted, that processing must be 'strictly necessary for the law enforcement purposes' (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 security Section 31 DPA). The ICO provides guidance as to these matters.

Proportionality

- 3.78. Where determining the proportionality of use of LFR, the seriousness of the circumstances to be addressed and intended outcomes being pursued should be balanced against the risk of intrusion on the rights of citizens. Any deployment should not be allowed to continue longer than is necessary to achieve the intended outcomes.
- 3.79. Proportionality is not only about balancing the effectiveness of LFR over other methods but of explaining why the particular technique or tactic is the least intrusive necessary to achieve the desired aim. This critical judgment can only properly be reached once all other elements and risks inherent in the intended LFR operation have been appropriately considered.
- 3.80. The potential for intrusion arising from LFR in certain uses could be argued to be similar to that arising from some forms of covert surveillance tactics and capabilities. The view of the SCC is that the elements of proportionality which are provided within the "Home Office Code of Practice for Covert Surveillance and Property Interference," should be the test which is applied by police decision makers when determining the proportionality of police surveillance conduct using LFR. That test is as follows:
- a) balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
 - b) explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others to achieve the desired purpose;
 - c) consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;
 - d) evidence as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

- 3.81. LFR technology impacts upon the Article 8 rights of any member of the public whose image is momentarily captured by it for comparison with images on a watchlist, even where an image is instantly discarded when no match is indicated by the system. This is the case even though such intrusion may be considered as being “negligible” in terms of that impact.
- 3.82. Recognising the intrusion impact where LFR may capture and process the images of large volumes of innocent people, an impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication. The balancing exercise which the principle of proportionality requires is not a mathematical one; it is an exercise which calls for judgement.
- 3.83. The SCC recommends that judgement is applied to the question of proportionality by an officer of appropriately senior rank in, consideration of the provisions of paragraph 4.6 to 4.19 in this guidance. Wherever LFR is being operated by the police, safeguards should be put in place to ensure that whenever the relevant case of proportionality changes for of the operational conduct, that an appropriate review is conducted by the police decision maker as to whether the operation should continue within its original terms or whether it should cease. In the interests of greater transparency and integrity, the SCC recommends that Chief Officers should enable decision making by the senior police decision makers to be made available for scrutiny by the local Ethics Committee structures. (Paragraph 2.25).

Risk Assessment

- 3.84. The assessment of risk and implementation of risk mitigation measures are fundamental ingredients of all police operations. Many thematic assessments of risk are required of the police by different statutes, some may be additionally required by organisational rules. The professional assessment of risk enables those senior police officers approving and leading police operations to make balanced judgements as to the legitimacy, legality and proportionality of their proposed or ongoing conduct.
- 3.85. The SCC acknowledges that the various demands associated with risk assessment completion may often give rise to duplication of effort as the police may frequently have to record the same or similar information, several times in different forms. They must keep the contents under review to amend as necessary throughout their intended conduct depending upon the requirements of any particular risk assessment undertaking. By means of illustration, as part of their intended LFR surveillance conduct, the following may apply to varying degrees (not a definitive list);
- An Equality Impact Assessment
 - Data Protection Impact Assessment
 - Self-Assessment Tool
 - Community Impact Assessment
 - Collateral Intrusion Risk Assessment
 - Privacy Impact Assessment
 - An Operational Risk Assessment

- 3.86. **The SCC recommends that the Home Office, regulators and other stakeholders collaborate to consider the development of a single ‘integrated impact assessment’ process/format which provides for a comprehensive approach to such matters. This is to improve focus, reduce duplication, reduce bureaucracy and avoid gaps whilst fulfilling statutory and organisational requirements in so far as they relate to the use of biometric and other surveillance enhancing technologies as part of a surveillance camera system including, but not exclusive to LFR.**
- 3.87. In order to give proper consideration to collateral intrusion and other associated risks, senior police officers who approve police conduct using LFR should fully understand the capabilities and sensitivity levels of the technical equipment which is intended to be used. Such understanding should then be applied in the context of what is sought to be achieved and the “5WH” specifics regarding deployment as described in preceding paragraphs of this guidance. In particular there should be an appropriately detailed understanding as to the potential for inaccuracy, error or bias within the relationship between the LFR technology, the human decision maker and police intervenors and a plan documented as to how these matters are to be effectively addressed.
- 3.88. When considering the nature and extent of risks associated with the use of LFR integrated with a surveillance camera system, particular regard should be given to those risks which are associated with cyber security. An assessment of cyber related risks to the security of data is also a requirement of the DPA 2018.
- 3.89. As well as addressing the broader spectrum of human rights considerations at risk of being infringed by the LFR technology, risks associated with the criminality being investigated, the compromise of police officers or police operations and those operating in partnership with them, the compromise of operational and evidential integrity, security breaches by ‘hackers’ who may seek to exploit vulnerabilities are examples of important considerations to be addressed. (See paragraph 5.12 Handling of Material).
- 3.90. Surveillance camera systems should be secure by design, and secure by default. These matters should be documented as part of a broader risk assessment approach.
- 3.91. **The SCC recommends as good practice, that when procuring LFR systems an assessment is made as to whether the software or hardware which is to be/has been procured and is to be used, has a known vulnerability, or history/pedigree of vulnerability to being ‘hacked’. Firewalls, anti-virus and other risk mitigation measures should be addressed particularly if the system is to be networked or cloud storage considered. Standalone systems are not immune from cyber vulnerability particularly if ‘pen drive’ or other image/data transfer media are to be permitted. Operational disciplines should ensure that processes are appropriately cognisant of cyber risks and staff using the system should be aware of those risks and how to mitigate them.**

4. Governance, Approval, Watchlists, Protected Characteristics and the Human Decision Maker

Governance

- 4.1. Chief Officers should ensure that there are effective governance arrangements in place which in turn ensure that LFR is lawfully and ethically operated in a manner which is transparent and accountable. Good governance also helps to engender and maintain the trust and confidence of communities.
- 4.2. Police and Crime Commissioners (PCC) (the Mayor's Office in London) are fundamental to the governance framework applicable to the operation of LFR by the police. They have a democratic mandate to be the voice of their communities, to enable the capabilities of their police force and to hold the Chief Officer to account. (See Section 7 – Accountability). In the context of LFR, the SCC considers it important for the PCC to be appropriately engaged and influential with those decisions which are within their statutory gift to make, particularly (but not exclusively) those associated with procurement, public engagement, performance and accountability. The SCC considers that the PCC should be engaged where the police seek to operate LFR by means of partnership arrangements with other organisations, whether collaborating in the use of LFR systems which are owned/operated by a partner agency (whether from the private or the public sector) or operating systems of their own. (See paragraphs 4.70 to 4.76 – Partnerships). Chief Officers should ensure that the PCC is meaningfully engaged at an early stage in these matters.
- 4.3. The SCC acknowledges the work of the Biometrics Institute; The 'Three Laws of Biometrics', as being informative for those seeking to develop a strategic framework with which to guide their approach to using biometric technology responsibly and ethically. The 'Three Laws of Biometrics' summarise at a high level a more detailed 'Good Practice Framework' which the institute has developed for its members. It is designed to assist with the planning and implementation of systems and, importantly, sets out the order in which tasks should be carried out (policy first, then process and only after robust review should use of the technology be explored). It provides a systematic pathway to help formulate sound policies and processes while considering their potential societal impacts. The key elements are as follows (a link to the Biometric Institute web site also appears below);
 - a) POLICY – comes first: Any use of biometrics is proportionate, with basic human rights, ethics and privacy at its heart.
 - b) PROCESS – follows policy: Safeguards are in place to ensure decisions are rigorously reviewed, operations are fair and operators are accountable.
 - c) TECHNOLOGY – guided by policy and process: Know your algorithm, biometric system, data quality and operating environment and mitigate vulnerabilities, limitations and risks.

<https://www.biometricsinstitute.org/>

Senior Responsible Officer

- 4.4. Although not a statutory requirement of PoFA, Chief Officers have previously confirmed to the SCC that they have designated a Senior Responsible Officer (SRO) in their respective forces so as to ensure that their responsibilities regarding PoFA and the SC Code have the appropriate strategic oversight. The SCC urges Chief Officers (who are the ‘relevant authority’ as described under the terms of PoFA) to consider aligning senior leadership responsibility for the LFR capability in their particular force to their SRO. The SCC suggests that clear decision making structures are established at an appropriate level of seniority and in support of the role of the SRO, which ‘approves’ any police operational conduct which is to make use of LFR, in consideration of the broad spectrum of legal and organisational responsibilities which arise from such conduct. In that regard the SCC highlights what he considers to be a good practice approach at paragraphs 4.6 to 4.19 below. The SRO may be distinct from an “approving officer” in that they are designated by a Chief Officer as having overall organisational responsibility for strategic organisational oversight, rather than statutory and operational/ tactical decision making in the context of specific police operational activity. These are entirely matters of good practice for a Chief Officer and not a requirement of law. The responsibilities of an SRO are recommended as follows (not an exhaustive list):
- a) the integrity of the process in place within the organisation for compliance with statutory, procedural and regulatory obligations,
 - b) effective coordination of senior members of the force with statutory responsibilities arising from the use of LFR (e.g. force Authorising Officer, Data Protection Officer, Data Controller, force solicitor etc.),
 - c) public engagement and communication,
 - d) arrangements for identifying, learning from and reporting of errors to the relevant regulators, and the implementation of processes to minimise repetition of errors (e.g. RIPA),
 - e) engagement with independent regulators where applicable, and
 - f) where necessary, oversight of the implementation of any action required by a regulator.
- 4.5. Surveillance activities by the police using LFR are by their nature, ethical, operational and organisational considerations as well as being considerations of law. It is recommended good practice that the SRO is engaged with the Chief Officer and PCC in decision making by the organisation to procure LFR technology in the first instance and also a party to those decisions as to the nature of the equipment procured. Consideration should be given to any operational and technical standards which have relevance to that system and the Public Sector Equality Duty (PSED) which arises in such matters, as addressed in earlier sections of this guidance. A list of national accreditation standards which are applicable to CCTV and surveillance cameras is held on the SCC site and is accessible by the following link:

<https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry>

Approval

- 4.6. It is important for the reader to note that the provisions of paragraphs 4.6 to 4.19 which follow below are simply recommended as good practice. They are not a requirement of the law, the SC Code or PoFA. The detail within these paragraphs is simply offered by the SCC as suggestions for Chief Officers to consider, where they are seeking to establish a governance framework for decision making which is consistent, transparent and demonstrates additional integrity of approach. Over and above the statutory responsibilities which set out decision making structures relevant to any particular legislation (e.g. RIPA, DPA), decision making ought to be of appropriate seniority in the organisation and should ensure that police conduct using LFR is approved, focused and kept under review within the context of the breadth of legal, organisational and operational considerations that apply to such use. Beyond any specific requirements of particular legislation, such arrangements are entirely a matter for the Chief Officer.
- 4.7. In particular, when considering the breadth of statutory responsibilities, the public interest equities and the applicable organisational/reputational factors which are inherent in police LFR activity, the SCC considers that the decisions which set the specific parameters for the relevant police operational conduct, and keeps such conduct under review are more demonstrably legitimate and transparent when addressed by appropriately senior officers who have a degree of independence from the operation itself. Within the obvious constraints of police structures the provision of a firewall between strategic decision makers and operational actors may also help the police to demonstrate a greater degree of integrity and operational independence in their specific decision making. Such a recommended undertaking is in addition to those arising from the PSED and those which arise in the context of personal data from the DPA 2018.
- 4.8. Although not a requirement of the Surveillance Camera Code of Practice, the SCC recommends as being good practice that, in a similar vein to the statutory role of Authorising Officer (RIPA), an officer of appropriate seniority in the organisation and who is not involved in the day to day direction of the LFR operation, should be designated as having responsibility for the “approval” of police operational conduct using LFR and for keeping such use under review. In particular the SCC recommends that senior officer approval is applied to the following matters as a minimum;
1. The approval of watchlists (including any subsequent changes made to it),
 2. The approval of the ‘similarity threshold’ applied to the LFR system (and subsequent changes to it),
 3. The coordination of those who have responsibilities for statutory undertakings e.g. PSED, DPA, PoFA, RIPA etc. and other assessment of risk in connection with the conduct,
 4. The establishment and approval of the specific (5WH) parameters of operational conduct using LFR (including any subsequent changes) together with the processes associated with reviews of ongoing conduct.
 5. The establishment of procedures and policies which keep the operational conduct under regular review and sets out the safeguards applicable to deciding who is to be placed upon a watchlist and where the technology will be used, and how those safeguards are to be applied.

- 4.9. The SCC recommends that such an undertaking extends to approving police activity which is to be conducted using the LFR systems which are operated by third parties in partnership with the police.
- 4.10. Officers approving LFR related conduct should endeavour to avoid approving operations in which they are directly involved, although it is recognised that this may be unavoidable particularly in the case of organisations with resource constraints, or where there is a need to act urgently.
- 4.11. Any approval which is granted should be based upon reasonable grounds and documented accordingly. The approving officer should also consider paragraph 3.87 in respect of the capabilities of the technology being approved.
- 4.12. Those conducting activity as part of an “approved” LFR operation should be aware as to the extent of any approval given so they do not risk going beyond them. In reaching their decisions an officer approving the overt surveillance using LFR ought to additionally satisfy themselves as to the details suggested at Paragraph 4.26 (Subjects) and Paragraph 4.30 (images) below.
- 4.13. Where a Chief Officer decides not to follow the good practice guidance suggested by the SCC in respect of the governance of operational activity in the foregoing paragraphs, the SCC suggests that they should otherwise clearly set out in their policies the detail as to the arrangements they have otherwise introduced to address such matters.
- 4.14. (n.b. The term “Approval” is deliberately used in this context rather than “Authorisation” so as to avoid any potential for confusion between the good practice advocated by the SCC in respect of ‘Approving’ the overt use of LFR by the police, with the statutory responsibilities associated with Authorising Officers in the context of covert surveillance which arise from the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016).
- 4.15. **The SCC recommends that the Home Office and Government review the laws which govern the conduct of overt surveillance by the police where such surveillance conduct employs biometric or similarly intrusive technology.**
- 4.16. **The SCC recommends that in consideration of the observations of the Court of Appeal in the Bridges case at paragraph 118 of that judgement, that the Home Office and Secretary of State honour the commitment made in the Home Office Biometrics Strategy (‘Better Public Services Maintaining Public Trust’ (Chapter 3 pg. 13)) which was published in June 2018, to review and update the Surveillance Camera Code of Practice in collaboration with the Surveillance Camera Commissioner so as to take cognisance of the evolving nature of public space overt surveillance by agents of the state since its introduction in June 2013, including – but not exclusive to – the challenges presented by the use of technology.**
- 4.17. **In both of the above cases, the SCC recommends in particular that clear provision is made for ethical standards, equality, legality and the governance and accountability of operational and intrusive conduct.**

- 4.18. **The SCC recommends that the NPCC and the Home Office consider developing consistent approval and decision making structures which approves operational police conduct overtly using LFR and which takes in to account and coordinates the breadth of statutory, regulatory and organisational roles and responsibilities which are inherent in the police use of LFR. Such arrangements should include considerations which are applicable to watchlists, system probability thresholds, the specific parameters of approved operational deployments of LFR (including any subsequent changes) and processes of review. In particular the SCC recommends that the strategic and operational decision making should be made by an officer of an appropriately senior rank who is not engaged in the day to day direction of the operation in connection with which LFR is to be operated (similar to that which exists in the statutory context of RIPA where an authorising officer performs such a role), so as to demonstrate a higher degree of transparency, integrity and operational independence in such matters.**
- 4.19. Where LFR is deployed operationally there should be clear command and control structures in place and clear responsibility and accountability established and documented. There should be clear objectives established for the operational activity. Appropriate arrangements should exist which ensure that any deployment of LFR is maintained under review by a senior officer so that it is not inappropriately operated beyond the operational parameters intended or longer than necessary to achieve its intended purpose (“mission creep”).

Use of Images and Watchlists – The ‘Who’ question

- 4.20. The SC Code applies to the use or processing of images (paragraph 1.11 SC Code) including those associated with a watchlist. ‘Watchlist’ is simply a collective term attributable to the catalogue of facial images assembled by the police, to be used by the LFR technology for comparison against faces later captured by its cameras once deployed.
- 4.21. In consideration of the “Who” question it is important that the police ensure that safeguards are in place, and are reflected in their policies which guard against an ‘impermissively wide area of discretion’ afforded in the selection of those who are to be placed upon a watchlist and to the selection of the location(s) where the use of LFR is to take place (the ‘Where’ question). Such vulnerabilities in policy and safeguards where they exist, may place the police conduct at risk of being undertaken in a manner which is not in accordance with the law (paragraph 3.5). It is therefore of additional importance that the police develop better policies and safeguards in respect of these areas when considering future use of LFR. Guidance should be sought from police legal advisers in appropriate cases.
- 4.22. Policies should also address the safeguards which apply to decisions as to how additions to and removals from the watchlist are managed. Those policies should be made accessible by being published in the public domain and updated as and when necessary with due regard given to confidentiality as necessary, and any risk of unnecessarily compromising the operational effectiveness of lawful conduct.

- 4.23. A watchlist for one operation should not be transported between different operations simply because of convenience (for example due to its size/volume of images). The SCC is of the view that it is the application of the law to the operational intent in consideration of the risks that arise which helps determine the justification for the inclusion of those people who are sought, and those images which are to be placed on a watchlist for any given operational deployment.
- 4.24. Typically watchlists should be created for specific deployments in a manner which does not go beyond that which is justifiable. Individuals placed on a watch list may be;
- a) wanted by the police for arrest on suspicion of an offence,
 - b) wanted for arrest on warrant issued by the courts,
 - c) vulnerable persons who are sought by the police because of risk.
 - d) 'persons of specific police interest' which the police frequently term as being 'for intelligence purposes.' This category of person is dealt with separately in the below sections. (Paragraphs 4.45 to 4.49) (See also paragraphs 3.59 to 3.74)
- 4.25. There is currently no legal prescription as to the level of seriousness of the offences which are being investigated by the police, which would justify the overt deployment of LFR. Without being unduly prescriptive as to such matters, the SCC considers that within the existing legal framework the degree of intrusion inherent in the overt operation of LFR requires an equally strong and compelling case of necessity and proportionality to be made to justify its use. This subjective decision making should be addressed by the senior police officer approving the police conduct using LFR. (See paragraphs 3.75 to 3.83 above regarding Necessity and Proportionality).

Considerations regarding Subjects

- 4.26. Guiding Principle 2 of the SC Code provides that 'The use of a surveillance camera system must take in to account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified', and (at paragraph 3.2.1); "The right to respect for private and family life set out in Article 8 of the ECHR enshrines in law a long held freedom enjoyed in England and Wales. People do however have varying and subjective expectations of privacy with one of the variables being situational". In addition, Guiding Principle 12 requires; (at paragraph 4.12.2) 'system operators to have a clear policy to determine the inclusion of a ... known individual's details on a reference database associated with such technology.' The application of the relevant legal principles to determine who will be placed on a watchlist is a matter of judgement for police decision makers in any given circumstance. Such decisions ought to be based upon reasonable grounds and made in the context of the conduct to be undertaken and what is sought to be achieved by that conduct. Policies should be produced which set out the safeguards which are applied to police discretion in such matters. Consideration should be given to establishing mechanisms by which police decision making may be subject to scrutiny in accordance with the provisions of paragraph 2.25 above (Ethics Committees).
- 4.27. A careful approach is necessary to ensure that the police conduct is neither speculative nor disproportionate in any way. The specificity of approach to decision making should take in to account the nature of risks which are applicable to those on a watchlist, whether operationally or otherwise as they will not necessarily be generic in nature. For

example, there may be individuals being considered for inclusion on a watchlist who may have a vulnerability or who represent a particular risk, the nature of which may render the intended use of LFR to locate and arrest them as being disproportionate in the particular circumstances it is intended to use the technology. Those are matters of judgement for police decision makers. It is important that the police are able to demonstrate, and be accountable for their justification for the inclusion of people on a watchlist. Decisions should be based upon reasonable grounds which in turn are grounded in information and facts. Inconvenience of effort due to the volume of images selected is not a reasonable excuse for avoiding established principles of law.

4.28. The following considerations are amongst those which should be applied to the selection of subjects of the police surveillance conduct when using LFR, by those responsible for creating and approving the creation of a watchlist.

- a) The information/intelligence upon which the police intend to rely upon as justification for placing subjects on to the watchlist and the pressing need/legitimacy/compulsion to act using LFR.
- b) What is sought to be achieved by means of LFR to locate the subjects sought and the reasonable grounds for believing that persons on a watchlist will be located within the parameters of the proposed deployment of the technology.
- c) The rationale as to why the inclusion of subjects on a watchlist to be used with LFR technology is both necessary and proportionate to what the police seek to achieve. This may include for example the grounds upon which it is considered important to locate the persons sought in consideration of the threat/harm/risk posed to others unless they are located.
- d) Confirmation that an assessment has been made by an Authorising Officer or other suitably competent person as to whether the intended conduct using LFR or any aspect of its intended use requires an authorisation under the provision of RIPA.
- e) Confirmation that the inclusion of subjects on a watchlist in the circumstances intended does not give rise to the risk of conflicting with or compromising other police activity whether overt or covert regardless as to whether or not such activity is anyway connected with the proposed LFR operation.
- f) Whether an assessment has been made as to risks posed by or to the subject(s) to be included on a watchlist (violent, vulnerable, health hazard etc) in the event that the subject may be confronted by police officers if identified and located by LFR.
- g) Whether an appropriate assessment has been made as to the risks which arise from the statutory responsibilities which apply to the inclusion of subjects on a watchlist in particularly those arising from the PSED in respect of equality and DPA with regards personal data processing.

4.29. The above details should be recorded by the officer responsible for approving the watchlist.

Considerations regarding the Images

- 4.30. Where subjects have been approved for inclusion within a watchlist there are further considerations which should be applied to their images which are to be used.
- 4.31. The Forensic Science Regulator is responsible for setting standards for the use of forensic science in the Criminal Justice System which are applicable where any use of LFR may be adduced as evidence in judicial proceedings.
- 4.32. The definition of digital forensics includes imaging, image comparison, video processing and enhancement. Most operational deployments of LFR would not generally be considered from a forensic science perspective, as the aim is usually to enable an intervention in live time and not necessarily to capture evidence. However, if there is a possibility that LFR outcomes will be used in evidence then the provisions of 'The Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System' apply. (See paragraph 5.4).
- 4.33. Images used by the police may come from a variety of sources, for example custody images of previously convicted persons, photographs harvested from open sources of information, police surveillance photographs covertly taken, images provided by members of the public etc. Different sources of images may give rise to differing legal considerations and differing risk assessment considerations which should be applied.
- 4.34. The following are amongst the factors which it is recommended should be considered in respect of the use of images on the watchlist;
- a) Is clarity provided as to the legal basis upon which the police are to rely for possessing and using the image as part of an LFR watchlist? The Police and Criminal Evidence Act 1984 and aspects of the common law may provide some legal foundation in some circumstances. The advice of legal advisors should be sought by forces where any doubt exists. This is particularly important in cases where the images intended to be used include those of persons who are not convicted of an offence.
 - b) Has the provenance of the image been confirmed? In particular confirmation should be obtained that the image being used is actually that of the identifiable person being sought by means of LFR. It should be established how that confirmation has been obtained and an assessment made as to its reliability.
 - c) Has an assessment of risk been conducted as to the use of a particular image due to the nature of its source, particularly where the image is derived from a sensitive or third-party source and its use in the manner intended, may risk compromising the source of the image and exposing them to risk.
 - d) Is the image of sufficient quality for use with the LFR system, recent and a good likeness of the subject who is sought?
 - e) Have responsibilities which arise from the DPA 2018 in respect of the image been, or are they being addressed and recorded in a DPIA and a DP Controller policy document? (Refer to ICO for guidance regarding responsibilities which arise from the DPA 2018).

Protected Characteristics – Race and Gender

- 4.35. There have been well publicised and understandable concerns expressed regarding the potential risks associated with inconsistencies of accuracy by facial recognition algorithms, operated by the police. Particular concerns arise regarding imbalances of performance where the technology assesses the facial features of people from black, Asian and other minority ethnic communities when compared to algorithmic performance in the context of white European male facial features. Identifying the potential for such risk is an enduring responsibility which should be considered as part of the PSED, be addressed and recorded at every level of decision making regarding the creation of a watchlist and each ingredient of the police conduct using LFR. (See Section 2 for more detail regarding equality and the PSED and Section 6 regarding Public Engagement).
- 4.36. Similar concerns exist regarding the ability of algorithms to perform consistently across genders. Any potential risk to transgender people should equally be considered. It is important that the police are appropriately aware of any strengths and deficiencies inherent in their technology and include such deliberations as part of the PSED duty. The conduct of an equality impact assessment is a fundamental obligation of the police in such matters. The SCC recommends as being good practice that such assessments and details as to the broader application of the PSED are made available to the Police and Crime Commissioners and local Ethics Committee for scrutiny with due regard given to matters of confidentiality.

Protected Characteristics – Children, Missing and Vulnerable Persons

- 4.37. Due to the particular vulnerability of children and vulnerable adults, the processing of their biometric data/facial images, should be subject to careful application of the necessity and proportionality test by decision makers. Aside from the legal and obvious ethical issues which arise in such circumstances, there are additional factors of accuracy to consider where images of children are concerned. In particular, their facial features may still be evolving and therefore there may be an inherent risk of inaccuracy by the LFR system or human decision maker.
- 4.38. There is an important distinction to be drawn between people who are “missing” and people who are “vulnerable.” The two terms should not be routinely conflated as not all who are “missing” are necessarily and by default “vulnerable.” The view of the SCC is that in general persons falling within the above categories should not ordinarily be included on a watchlist for the purpose of LFR operations simply because they are “missing” i.e. their whereabouts are not known. The SCC anticipates that the images of children will not be included on a watchlist except in circumstances which are so, due to the inherent threat/risk/harm considerations which apply, as to make their inclusion justifiable in law as being both necessary and proportionate.
- 4.39. There should be safeguards established which ensures that the justification for the inclusion of images of children, missing and vulnerable people to remain on the watchlist is kept under review. An image should be removed from a watchlist as soon as it is identified by the police that no further justification exists for its inclusion.

- 4.40. The safeguards to be applied to the inclusion of images of young people should be recorded in police policies.
- 4.41. It is important to emphasise that the above criteria are simply an approach which the SCC considers to be good practice in such matters. In cases of urgency or high risk in particular, the application of the process should not delay unreasonably the operational process. The over-riding consideration for the police is for their conduct to be demonstrably legitimate, lawful, ethical and proportionate to what they seek to achieve.

Protected Characteristics – Ageing and Facial Changes

- 4.42. The process of ageing, i.e. in this context, the changes to the physical characteristics of a face between the time when an image is taken and when it is later to be compared by technology, may negatively affect the accuracy of LFR as facial features will naturally evolve over time. This should be borne in mind where facial images of people are to be compared to images of them which were taken many years earlier. In such circumstances the police should take all reasonable steps to ensure that they use the most recent and up to date image of the subject available to them which is of sufficient quality for use with LFR, AND assess the extent to which there may be any difference between the image to be used and the current facial features of the subject sought by means of LFR. Similar considerations may apply in circumstances where a person has undergone a cosmetic procedure on their facial features. Any decision to include an image in such circumstances should only be made after an appropriate assessment of risk has been conducted.

Protected Characteristics – People with Disability

- 4.43. Care should be taken where people with a disability are to be included within a watchlist. For example, where the subject has suffered a facial injury, undergone facial surgery, has a degree of facial trauma or is of a particular bearing which inhibits their facial features from being recognised by the LFR then a higher degree of risk may arise in respect of accuracy. The SCC expects that people with such disability would only be included within a watchlist in connection with such matters which make their inclusion on a watchlist justifiable as necessary and proportionate to a stated purpose and where no other reasonable options to identify and locate their whereabouts exists. It may be that more than one protected characteristic listed in the forgoing paragraphs may apply to any given image/individual and as such demonstrates the importance of individual and distinctly separate assessment by police decision makers.

Face Coverings

- 4.44. Where persons on a watchlist wear face coverings, (e.g. face masks worn for public health reasons, arising from pandemic or religious purposes etc.) it is important to assess whether or not any risk of inaccuracy arises from the capabilities of the LFR technology and/or the human decision maker and whether any such risk where it is found to exist may be compounded where the subject has protected characteristics.

Information Gathering and Persons of Specific Police Interest

- 4.45. The inclusion of persons on a watchlist who may be referred to as being ‘persons where intelligence is required’ is a matter which requires careful consideration as such a term is so broad that it could be applied to anyone who is of interest to the police. The specific safeguards applicable to police discretion in such matters should be established in police policies.
- 4.46. One particularly distinguishing factor applicable to persons who are of specific interest to the police, where the intention is to gather information about them by means of LFR, (and which distinguishes them from those otherwise sought for arrest and intervention by means of the technology) is that it is unlikely that the subject of the police surveillance conduct will become aware that they have been specifically targeted by the police surveillance conduct. They may not be stopped or otherwise spoken to by the police at or around the time that they have been highlighted by the technology to the human decision maker, as the police may not wish them to know that they are obtaining information about them at the material time.
- 4.47. It may be that the information sought regarding a person of specific police interest may be required by the police for their own purposes or the information may be gathered by the police on behalf of another organisation or other third party with whom they are working in partnership. In such circumstances, the potential arises for the police conduct to amount to being covert surveillance which may require a directed surveillance authorisation to be granted in respect of the intended conduct under the provisions of RIPA. It is a strongly held view of the SCC that wherever the police seek to use LFR in these circumstances, an Authorising Officer (RIPA) should first consider the full circumstances beforehand so as to determine whether an authorisation should be considered under the provisions of RIPA. There should be transparent safeguards applied which are addressed within the police policies that are published on such matters. The SCC recommends that watchlist images of people who are to be located by means of overt activity are separated from watchlists of images of persons who are to be sought by means of covert surveillance using an overt LFR system. Different legal, procedural and risk assessment considerations apply in each case.
- 4.48. In particular it should be determined whether or not there is a legitimate information requirement (i.e. a gap in the knowledge base of the police about a person which they need to address by means of gathering further information) the nature of which makes the use of LFR necessary and proportionate in those circumstances.
- 4.49. It is recognised that circumstances occasionally arise where the police need to locate a person who is not suspected of committing any crime but where they need to act in order to prevent or detect crime, or to protect an individual from harm. For example; a person whose location is sought may unknowingly be the subject of a credible threat or otherwise at risk of harm which the police are seeking to avert (such as kidnap or serious assault), be a victim of a serious crime (for example a sexual assault) whose whereabouts need to be urgently established, or the locating of a person may be necessary to prevent or detect crimes (for example a known associate of an offender who has committed, or is about to commit a serious crime or is a witness to such a crime). Where the use of LFR is contemplated in such matters, the view of the SCC is

that the relevant circumstances should be of such seriousness as to justify the intended police conduct as being lawful, necessary and proportionate to what the police are seeking to achieve by means of LFR. Such matters are for police decision makers to determine on the basis of reasonable grounds and the application of the law, on a case by case basis. The provisions of paragraph 4.28 may assist in that regard. Decisions should be recorded together with the supporting rationale and be capable of being held to account by third party scrutiny as necessary.

Intelligence

4.50. An algorithm does not provide a definitive identification of an individual, it provides an indication of likeness between images together with a “similarity score”. Where the information is obtained about an individual by means of LFR regarding a person of specific police interest, and is to be recorded on an information or an intelligence system, care should be taken not to suggest that the subject has been ‘identified’ by LFR, unless the identity of the relevant person has been confirmed by other means (in which case those means should be clearly set out). It is good practice to ensure that the provenance of the information/intelligence to be recorded on an information/intelligence system appropriately reflects that a **similarity** rather than an **identification** arises from LFR in respect of an image held on a watchlist, together with any similarity score produced by the system in respect of that image. Other factors such as the reliability/accuracy of the technology should also be a consideration when evaluating the intelligence/information. In so doing, any subsequent assessment/analysis/decision making and action conducted by the police, and others, which relies on the accuracy of the information/intelligence obtained (in whole or in part) may be more reliably considered. It is for the police to determine whether there is the need to consider providing further guidance with regards to the recording of intelligence derived, whether in whole or in part, from the use of LFR.

Other Considerations

- 4.51. The following is a list of additional considerations which the SCC recommends should be applied by police policy makers in respect of watchlist compilation;
- a) Has an equality impact assessment been undertaken in respect of those on the watchlist? In particular has a sufficiently detailed assessment been undertaken as to the capabilities of the LFR system to be used to the extent that the police are satisfied that there are no undue risks of ‘bias’ within the system or human decision maker function and has this been documented? (See paragraph 4.52 – Human Decision Making).
 - b) Are processes in place which keep the performance of the LFR system and human decision maker under operational review and ensure that any changes to the original assessment are identified and acted upon in a timely manner?
 - c) Consideration should also be given as to establishing the required quality of an image to be placed on a watchlist which should be sufficient to maximise the potential of the system providing an accurate indication of likeness of the subject whilst minimising risk associated with an error being provided.
 - d) The police should be in a position to provide meaningful information relevant to images on a watchlist which are of relevance to the PSED.

- e) Is the size of the watchlist and the quality of images used proportionate to the legitimate objectives of the operation and within the capabilities of the LFR system?
- f) Suitable arrangements should be put in place which ensure that any changes to a watchlist (such as any subsequent addition of new images, removal of any images or replacement of an existing image with a different image of the same subject) are appropriately considered and approved. Those arrangements should be approved by the senior officer with watchlist oversight responsibility. In particular the police should be alert to any potential for ‘mission creep’ (original objectives being changed) occurring by the inclusion of additional images, and processes ought to be put in place to prevent such an occurrence.
- g) Appropriate co-ordination should be established by the operational leaders as necessary within a police force e.g. with the relevant Covert Authorities Bureau so as to ensure that there are no risks of compromise or ‘blue on blue’ activity taking place as a result of the LFR operational activity.
- h) Responsibilities which arise from the DPA 2018 in respect of the watchlist have been, or are being addressed and recorded in a DPIA and a Data Controller policy document and an assessment of risks to the rights of citizens enshrined within the ECHR has been made. (Refer to ICO for guidance regarding responsibilities which arise from the DPA 2018).
- i) The safe guarding of the images used to create a watch list is the responsibility of the implementing authority, the risk assessment should identify and address the key issues.
- j) The policy or procedures regarding the use of images should include who has access to the images in any form including paper and electronic, as well as storage, transfer and effective removal of images from any system they are introduced onto once their legitimate use expires (this includes but is not limited to thumbnail cache).

Human Decision Making

- 4.52. The SC Code makes it clear (paragraph 3.2.3 SC Code) that when LFR is operated, it “should always involve human intervention before decisions are taken that affect an individual adversely”. In addition, Article 22 of the GDPR and Article 11 of the Law Enforcement Directive generally forbid automated decision making (refer to ICO for further guidance).
- 4.53. A fundamental ingredient of the lawful use of LFR as part of a police operation is that there can be no decision making by the technology. Decision making should only be made by a human decision maker and not an algorithm. It is important to acknowledge that ingredients that are key to **human recognition** may not be the same factors applied by LFR algorithms when determining **recognition by the technology**. The SCC acknowledges that the ingredients that are key to human recognition may not be the same factors applied in an LFR system to establish “recognition.” There is a risk that a subject’s face, including any changes in facial features, may be judged differently by a human than by the technology.
- 4.54. LFR algorithms do not provide a confirmation of identification of a person when highlighting similarity between an image captured by the system with an image held on a watchlist.

- 4.55. An algorithm simply does what is asked of it within an LFR system and that is simply to provide an indication as to the likeness between images and the provision of a similarity score which indicates the algorithmic assessment as to the extent of similarity between those images. In so doing, the system enables a human decision maker to consider and evaluate this information themselves and thereafter to make a considered decision based upon all relevant information in their possession. Usually that decision is to determine whether there are reasonable grounds to believe that the two images may be of the same person or are otherwise sufficiently similar in facial characteristics to the extent that police action is justified in respect of the person indicated. Ordinarily that decision is likely to be for a police officer to intervene and speak with the person identified by the system. In the first instance this may be with a view to confirming the identity of a person before deciding upon any other action necessary.
- 4.56. Whilst there has been a good deal of discussion and concern about the potential of a bias with LFR technology arising from inconsistency, the view of the SCC is that there has not been the necessary depth of discussion or derived understanding, as to where such risk exists within the police arrangements as a whole, and to what extent, if any, the role of the human decision maker may be a factor. As a minimum undertaking the SCC recommends that clarity is provided as to the human decision maker function in every operational deployment of LFR and is suitably addressed within police policy documents by decision makers. Safeguards which ensures that arrangements are not 'ad-hoc' and which determine whether decision making is to be made by a single or group of decision makers, whether those arrangements change during the course of an operation, how decisions are made and recorded and subsequently analysed and assessed/reported for consistency and efficiency, are all matters for senior police decision makers to address.
- 4.57. The SCC recommends that senior officers should ask themselves how they select, train, instruct, deploy, manage and analyse the performance of the human decision maker, as part of their operational conduct and that the answers should be documented as part of the PSED.
- 4.58. It is good practice for the police to have clear policies, guidance and safeguards in place which ensure that human decision making is transparent, balanced and fair, as well as being resilient to any risk of bias or inconsistency. Suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must also be in place.
- 4.59. Human decision making should be meaningful and guard against a tendency to defer to an algorithm by simply agreeing with or endorsing all outcomes of the LFR system. To do so would simply be to render decision making as being essentially automated.
- 4.60. On the other hand, if human decision makers regularly and routinely reject indications provided by the system, this may give rise to a question as to the efficacy of the technology itself and indeed the decision maker.
- 4.61. Human decision makers should be alert to the possibility of suggestion that they may be more inclined to accept or overrule an indication made by LFR where the indication is in line with any stereotypes they may have. Consideration should be applied to the capabilities and competency of the human decision maker and any risks which may arise from unconscious bias.

- 4.62. The human decision maker should be appropriately aware as to how the LFR system works, the extent of its capabilities and any possible risk of inconsistency associated with recognising individuals amongst the diversity of the subjects on the watchlist and amongst the population being subject to surveillance.
- 4.63. The human decision maker should be alert to any circumstance whereby the surveillance activity being conducted using LFR may amount to being covert surveillance and take appropriate action.
- 4.64. The human decision maker should be alert to any particular trend developing during an operation which may give rise to questions of accuracy and take appropriate action. The SCC recommends that it is good practice for police post operational review processes to include the performance of human decision making/adjudication so as to inform future conduct.
- 4.65. **In recognising the quality of their work in respect of digital ethics, the SCC recommends that the College of Policing and the NPCC consider whether at a national level, the role of the human decision maker should be better defined, “structured” within a surveillance camera system, benefit from further nationally produced guidance or training and the role quality assured by means of meaningful analysis of performance. Such standards where they are established should be consistent across different police forces/organisations and for Chief Officers to have regard. In any event it is good practice for there to be measures in place which quality assure and demonstrate the performance of human decision making associated with LFR. This information may be made publicly available as appropriate.**

Similarity Threshold

- 4.66. The establishment of a “similarity threshold” within LFR and its application to images held on a watchlist are considerations which are integral to the accuracy, proportionality, justification and assessment of risk for the police use of LFR. The SCC recommends that decisions which establish the similarity threshold for police conduct using LFR should be made or approved by the senior officer with responsibility for approving the watchlist and LFR operation (paragraph 4.6). The similarity threshold informs the algorithms as to the level of similarity/likeness required between images captured and analysed by them against those held on a watchlist, for which the human decision maker requires notification. In essence the similarity threshold widens or narrows “the police surveillance net” depending upon how it is set and thereby influences the potential for persons to be wrongly captured by it.
- 4.67. Where the threshold is set to a high level of similarity then fewer indications of likeness may be produced for the human decision maker to consider and therefore rates of subsequent identifications of people made by intervening police officers may be proportionately higher. In contrast, a lower threshold of probability is likely to produce the opposite outcome. The level of similarity threshold set on a system may be changed depending upon the particular circumstances of an operation and is a matter of professional judgement applying the principles of proportionality on a case by case basis. In general, the levels of similarity to be applied will be commensurate with the risks and vulnerabilities associated with each case.

Statutory Collaborations

4.68. Sections 22A to 23I of the Police Act 1996, as amended by the Policing and Crime Act 2009 and the Police Reform and Social Responsibility Act 2011 enable Chief Officers of police to make agreements about the discharge of their functions. Sections 22B and 22C of the 2011 Act place duties on Chief Officers and policing bodies to keep collaboration opportunities under review and to collaborate where it is in the interests of the efficiency or effectiveness of their own and other police force areas. Home Office guidance as to these matters is accessible at the below link;

<https://www.gov.uk/government/publications/statutory-guidance-for-police-collaboration>

4.69. The SCC recommends that Chief Officers consider whether any of their functions which arise from PoFA and the SC Code in respect of the lawful operation of LFR may be addressed under the collaboration provisions and take any action as they consider appropriate within the terms provided by the legislation. Police and Crime Commissioners should be engaged in such decision making.

Partnerships and the use of Third Party Owned/Operated Systems

4.70. The provisions of paragraphs 4.70 to 4.76 below concern situations of contractual agency in connection with which Chief Officers may wish to seek legal advice in appropriate cases. Where the police work in partnership with other organisations in the operation of LFR, such partnership arrangements may involve third party organisations working alongside the police in respect of a police owned/operated LFR system for a shared legitimate purpose. Alternatively, the police may seek to work with a third-party owner/operator of an LFR system which they wish to be operated in a manner which supports a legitimate policing (law enforcement) purpose. The duty to have regard to the SC Code still applies to the police in respect of the discharge of relevant functions covered by the SC Code in respect of the system being operated. Those responsibilities arising from the SC Code do not apply to third party operators by virtue of law unless they are designated as being a 'relevant authority' in accordance with PoFA (however, see paragraph 4.76 below). The DPA applies to all parties.

4.71. The statutory responsibilities which befall the police arising from the SC Code extend to the operation of a third party owned system to the extent that it is being used to support a police requirement and therefore extends to any such overt use of a private (or other agency owned public) LFR system.

4.72. Paragraphs 1.11 and 3.4.2 SC Code illustrate that it is for the police to ensure that any third-party system being operated in support of them as part of a partnership, accords with the provisions of PoFA where it is so used, the responsibility for which lies with the police. Third party private sector service providers or other private entity partners are not under a duty to have regard to the SC Code. That duty rests with the police to ensure that systems used on their behalf are so used in a manner which is compliant with their statutory duties. The police should be able to demonstrate that they are acting lawfully, with integrity and not vulnerable to suggestions that they are exploiting LFR capabilities 'by a back door' (unlawfully), in using the biometric capabilities of others for their own purposes.

- 4.73. Where the third-party operation of a surveillance camera system is being conducted by a private sector contracted service provider, the police should ensure that any contract which relates to the operation of that system places a contractual obligation on the supplier to act in accordance with the provisions of the SC Code and relevant statutory provision whenever that system is being operated in partnership with, or at the request/behest of the police.
- 4.74. It is a requirement of the SC Code that where a system is jointly owned or jointly operated with or by the police, the requisite governance and accountability arrangements should be agreed between the partners and documented in a protocol so that each of the partner organisations has clear responsibilities, with detail provided as to obligations and expectations, and the procedures agreed for the resolution of any differences between the parties or changes of circumstance.
- 4.75. To summarise these considerations more specifically; The police are responsible for ensuring that a surveillance camera system being operated by a third party in partnership with or in support of the police for a legitimate purpose, is being so operated in a manner which accords with Section 33(1) PoFA and be validated as being so operated with regard to the SC Code at any time that the system is being operated in partnership with or otherwise at the behest of the police. In each case the relevant police force should seek the guidance of their force solicitor, the force Authorising Officer and Data Protection Officer as necessary. Decisions should be recorded and appropriate safeguards produced in publicly available police policy. These provisions are equally as applicable to the surveillance camera systems and relevant actions of local authorities and indeed all **relevant authorities** as prescribed by Section 33(5) PoFA.
- 4.76. The SCC urges all those agencies who work together in a partnership using LFR ,to aspire to the highest ethical, procedural and legal standards which exist across the organisations and to a consistent level. This is of additional importance where the police operate with private sector bodies whose surveillance conduct is regulated to a different legislative and regulatory standard than the police. Particular caution is urged where a third party LFR system contains high volumes of images whether their own or as provided by the police. Regardless of those volumes, the police ought to guard against any risk of simply “adopting” a pre-prepared third party watchlist or provide images for use in connection with such systems without approval by police decision makers, regardless as to the volume of those images to be used by a third-party system at their behest. In addition, the SCC recommends that a third-party operator of a security camera system which uses LFR in partnership or otherwise at the behest of the police and who is not a relevant authority as prescribed by PoFA, voluntarily adopts the provisions of the SC Code and its Guiding Principles, as recommended at paragraph 1.17 of the SC Code. As a matter of good practice, the SCC recommends that the question as to whether a third-party system operator voluntarily adopts the SC Code should be explicitly addressed in the documented protocol agreed between partner agencies. It is also good practice to place the documented protocol which addresses these issues (whether a service level agreement or memorandum of understanding etc) in the public domain whilst maintaining confidence as to matters of sensitivity and security.

Operational Trials

- 4.77. Whenever the police seek to conduct operational trials using LFR it is important to recognise that the statutory responsibilities which apply to the police conduct and use of LFR remain in their entirety, including those relevant to the handling of material and are in no way diluted simply because the police choose to categorise their conduct as being a trial. The SCC considers that meaningful engagement with communities and the provision of relevant information to the public (including information about success and about failures) are essential ingredients of any successful trial of police overt surveillance camera systems. Separate considerations and safeguards apply in respect of covert applications, which are regulated by the Investigatory Powers Commissioner.
- 4.78. **Before** any trial activity commences consideration may meaningfully be applied to informing the public as to what in particular is being trialled (e.g. the equipment, a component of the equipment, the police structures or policies regarding the equipment etc) and to what end (purpose). It is also helpful for the police to be clear as to when trials will start and end and what the police consider success to look like.
- 4.79. The purpose of a trial should be driven by the end user requirement. The end-user requirement should include recommendations from regulators (e.g. SCC, Forensic Science Regulator, ICO) as well as functional requirements regarding such matters as accuracy. The outcome of the validation is to define what a method (or the output of a method) should be used for, if any risks persist and any caveats that might apply, e.g. error rates. Only when evaluation of the trial has shown the method is fit for purpose (the purpose is defined by the end-user requirement) using test subjects whose identities are known to the evaluator, should the method be considered suitable for live trials and/or piloting. The results of trials and pilots should be objectively evaluated and appropriately communicated to the public. A clear methodology of evaluating the system should be established and communicated at the outset as part of this undertaking. (See also paragraph 5.5).
- 4.80. The SCC has developed a 'passport to compliance' document which sets out a staged approach to consider when planning, implementing and operating a surveillance camera system so as to ensure it complies with the SC Code:

<https://www.gov.uk/government/publications/passport-to-compliance>

5. Integrity, Use of Material as Evidence and Handling of Material

Digital Integrity and Forensic Standards

- 5.1. Material which is used in connection with or derived from the use of LFR is capable of amounting to being information, private information, metadata, data, personal data, intelligence and evidence. Each category of material has to be separately considered and is subject to several and separate legal and regulatory applications depending upon its nature and intended use.
- 5.2. It is important that there are effective safeguards in place to ensure the integrity of recorded information and its usefulness for the purpose for which it is intended. The Code of Practice for the Management of Police Information (MoPI) is relevant and is accessible via the below link.

<http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf>

- 5.3. The Forensic Science Regulator is responsible for the regulation of digital forensic standards which are applicable to the use of surveillance camera systems including those which involve facial recognition algorithms. The wider forensic considerations which may apply to LFR include (amongst other considerations) the equipment, the processes, the management of a watchlist and LFR system, handling of material and production/continuity of evidence.
- 5.4. “The Codes of Practice and Conduct, Standards for Forensic Science Providers and Practitioners in the Criminal Justice System” is provided by the Forensic Science Regulator in respect of digital forensic matters and is accessible by means of the following link:

<https://www.gov.uk/government/publications/forensic-science-providers-codes-of-practice-and-conduct-2020>

- 5.5. The Forensic Science Regulator has also developed a helpful guide which illustrates each stage of a process which may be followed when seeking to “pilot” LFR or similar technology. (See Appendix C).

Evidence

- 5.6. Material obtained by means of the overt use of LFR enhanced surveillance cameras may be used as evidence in judicial proceedings. The admissibility of evidence is governed primarily by the Common Law, the Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

- 5.7. The continuity and integrity of evidence are critical to every prosecution and are applicable considerations as part of the disclosure regime under the Criminal Procedure and Investigations Act 1996. The police should be able to demonstrate how evidence has been obtained and also demonstrate their adherence to the statutory responsibilities placed on them to the extent required by the relevant rules of evidence and disclosure.
- 5.8. Where the product of LFR enhanced surveillance cameras could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In particular, attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996 (CPIA), which requires that the investigator retain all material obtained in an investigation which may be relevant to the investigation. The Code of Practice (CPIA) may be accessed by means of the following link.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf

- 5.9. Any failure on the part of the police to have regard to the SC Code as required by Section 33(1) PoFA in respect of the use of LFR in proceedings similarly is a disclosure consideration. Attention is drawn to the following extract from the CPS disclosure manual (pg. 80):

“Use of Surveillance Camera Systems by Police Forces.

The use of overt surveillance camera systems in England and Wales is covered by the Surveillance Camera Code of Practice which is overseen by the Surveillance Camera Commissioner. The relevant legislation is s33 Protection of Freedoms Act 2012.

This Code covers the use of surveillance cameras in public places, police operated CCTV systems and body worn cameras. Where the police seek to rely on images derived from such surveillance cameras, Prosecutors should enquire whether the cameras are code compliant. If the cameras are not compliant with PoFA and the Code, then this non-compliance may fall to be disclosed under the requirements of CPIA.

It should be stressed that non-compliance is highly unlikely to render the material inadmissible but the prosecutor ought to be aware of the disclosure implications.”

- 5.10. The CPS disclosure manual is accessible via the following link:

https://www.cps.gov.uk/sites/default/files/documents/legal_guidance/Disclosure-Manual-12-2018.pdf#page67

- 5.11. The Code for Crown Prosecutors can be accessed at the following link:

<https://www.cps.gov.uk/publication/code-crown-prosecutors>

Handling of Material

- 5.12. Senior officers, through the relevant Data Controller, must ensure compliance with the applicable
- a) data protection requirements under the Data Protection Act 2018 and ensure that any relevant internal policies produced by the police force relating to the handling, dissemination, storage and destruction of material are complied with. In particular the police should ensure that appropriate security measures are in place which;
 - b) Protect the operational security of police conduct and procedures;
 - c) Provide appropriate levels of document classification and physical security to protect any premises where material may be stored or used;
 - d) Provide appropriate IT security measures which mitigate risks of unauthorised access to IT systems;
 - e) Ensure an appropriate security and access regime for personnel which provides assurance that only those who require to have access to this material may do so and are reliable and trustworthy;
 - f) Are sensitive to the requirements of any third party with whom they work in partnership.
- 5.13. The SCC considers it good practice for the Disclosure Officer and the Data Controller (and Authorising Officer in appropriate cases) to liaise in respect of the management of material (whether to be used or un-used as evidence) so as to ensure that all applicable statutory responsibilities are properly considered and discharged. There are additional safeguards which arise from RIPA and the Investigatory Powers Act 2016 where material arises from the use of LFR in a covert context.

6. Public Engagement, Provision of Information, Performance

Public Engagement

- 6.1. There is evidence of a degree of public acceptance of LFR technology being used by the police particularly so in respect of matters which are considered by them to be serious matters. 'The Ada Lovelace Institute' ("Beyond Face Value; public attitudes to facial recognition technology". September 2019) appropriately illustrated that;

"There is no unconditional support for police to deploy facial recognition technology: rather support is conditional upon limitations and subject to appropriate safeguards."

- 6.2. Public support is not consistent across all communities and the police should guard against any temptation to consider otherwise, as members of diverse or vulnerable communities are likely to be more suspicious of police endeavours. Engagement with communities should be integral to any police operation using LFR. Such engagement should be meaningful and go beyond simply the production and distribution of information material. It is particularly important that the police make a distinction between "engagement" and "consultation" with communities. It is one thing to simply engage by providing information and entirely another to have an ongoing process of meaningful consultative dialogue, challenge, reflection and feedback. This is particularly important in the case of those who may feel disproportionately affected by police use of LFR, and their elected representatives as appropriate. For engagement to be meaningful it should involve a dialogue which is maintained as a continuum before, during and after LFR operations are conducted. Such issues should also be addressed as part of the PSED.
- 6.3. Chief Officers should ensure that their Police and Crime Commissioner is consulted at an early stage when developing their approach to community engagement. The police should be proactive in publishing relevant information which should include publishing their successes and failures and encourage feedback as appropriate from which they may derive further learning. Such matters may also be of relevance to the PSED which arises.

Provision of Information

- 6.4. The duty of the police to provide information in respect of their LFR activity is wide ranging and is not constrained simply to the arrangements they have in place to engage with their communities. For example, for the police to be seen to be acting 'overtly' there should be appropriate information prominently displayed, distributed or otherwise provided to the public which clearly informs the public that LFR is being operated by them or on their behalf. There are a number of good practice approaches which the police may also consider such as use of local press and media outlets, use of the police or third-party internet sites, social media accounts or indeed the establishment of a dedicated internet communication application etc.

- 6.5. One of the many benefits associated with the police proactively and meaningfully providing information to their communities about their use of LFR is that it enables people to make informed choices to protect their privacy, for example by taking action to avoid the area under surveillance by the police or to otherwise take action to guard their facial features from the LFR camera. There is a distinction to be made in terms of whether an individual's conduct in protecting their privacy from an operationally deployed LFR system is undertaken so as to protect their privacy and wider human rights, or is conduct indicative of suspicious behaviour relevant to criminality. This important distinction should be considered where police officers look to establish reasonable grounds to intervene and stop an individual due their conduct within the vicinity of an overt LFR deployment.
- 6.6. People who may be affected by the police use of LFR, whether because they appear on a watchlist or whether their image may have been captured and analysed by the algorithms operating, are entitled to an effective legal remedy. For example, people may wish to complain or challenge the police as to why their image has been used or captured in a manner which is not transparent or that they have been stopped by the police as a result of a shortfall in the way that the technology and the police have operated. The potential exists in such circumstances for an individual to suffer inconvenience which has adverse consequences for them (e.g. they may be made late for work or suffer reputational impact as a result of the police stopping them and calling them to account) and they therefore have the right to challenge all decisions and actions of relevance which have been made.
- 6.7. It is recognised that in being appropriately transparent, the legitimate interests of law enforcement and national security may in some circumstances require a degree of confidentiality to be applied in order to legitimately deliver effective lawful conduct. The provision of relevant information to the public is of fundamental importance to establishing and maintaining the public's trust in the conduct of the police. Matters of confidentiality are for police decision makers to determine. Decisions should be based on reasonable grounds and not on grounds of operational convenience. It is important that decisions as to confidentiality are capable of being held to account by relevant third party scrutiny where necessary, for example in judicial proceedings. Police policies and procedures should set out and inform the public as to the arrangements which exist and which enable the public to challenge any aspect of the police conduct. The information provided should include the relevant details of the police point of contact (including telephone number, email address and/or postal address) which should be engaged in the first instance and how they may obtain further information.

Performance Management

- 6.8. The SC Code explicitly recommends that operators of surveillance camera systems should be proactive in the provision of regularly published information about the purpose, conduct of operations and effect of a system (Paragraph 3.3.4 SC Code).
- 6.9. The production of up to date, accurate and meaningful information to the public regarding the operation, success and shortcomings of police activity should be an ingredient of any police conduct which involves the use of LFR. Such an approach is entirely consistent with the Government's commitment to greater transparency on the

part of public bodies. In particular the provision of relevant and meaningful performance information will help to inform and develop better understanding as to the integrity and legitimacy of police endeavours using LFR, enabling the public to draw their own conclusions on a more informed basis.

- 6.10. **The SCC considers that it would be beneficial for the NPCC to develop a meaningful and national suite of relevant performance indicators which demonstrates as a minimum, the purpose, successes, failures, outcomes, the nature and extent of intrusion and the accuracy and diversity of impact of their LFR operations. The SCC recommends that such a body of performance information should be developed in a manner which is nationally consistent amongst police forces in England and Wales and recommends that HMICFRS are appropriately consulted on such matters.**
- 6.11. **The SCC further recommends that the police should develop nationally consistent terminology attributable to the use of LFR systems. In doing so more meaningful analysis, comparison, understanding and learning may be derived by the police, the public and the wider stakeholder community.**

“False Positives and Negatives”

- 6.12. The SCC considers the terms ‘false positive’ and ‘false negative’, which have become normalised in terminology attributable to LFR both nationally and internationally, not to be particularly helpful nor indeed sufficiently accurate terminology. Specifically, the terms ‘positive’ and ‘negative’ are at least suggestive of the notion that the LFR system provides ‘alerts’ which are positive and negative identifications of individuals, whereas the algorithms provide a technological indication of similarity between images together with a similarity score. Of course, human decision makers determine police action in consideration of information provided by LFR and so “falsehoods of positives and negatives” are arguably as attributable to humans (police officers) as they are to the technology, and the public do not readily make this differential due in no small part to these unhelpful terms.
- 6.13. Paradoxically, in cases where LFR technology provides an indication of likeness of someone whose image it has captured and the human decision maker has sanctioned a police intervention, and it is then found that the person stopped is not the person whose image is on the watchlist but they simply have a degree of likeness to that image, then the system is arguably doing what it is set up to do – indicate strong similarities between facial images. In such circumstances the system may not therefore be providing ‘false’ ‘negative’ or ‘positive’ information. Operators should however be aware of alerts which appear to be clearly and significantly erroneous. The frequency or isolated nature of such an occurrence may be relevant to the enduring PSED in determining whether such instance arises from a characteristic of the technology and thereby amount to being a concern over accuracy.
- 6.14. When determining appropriate performance measures, the SCC considers that it is important to properly make a distinction between the components which make up the police operational system, for example the **purpose**, the **watchlist**, the **technology**, the **human decision maker** and the **police intervention and outcomes** and the context of equality and intrusion in which the technology is operated.

6.15. In developing an appropriate framework of performance information with which to inform the police and the public, the SCC suggests that it may be appropriate to consider the inclusion of the following themes in respect of which relevant and meaningful information could be provided. The below is simply offered as a suggestive but not an exhaustive, mandatory or definitive list;

1. The Purpose

6.16. It is acknowledged that there is a need to ensure confidentiality in the interests of the operational effectiveness of lawful conduct. However, where the purpose / requirement of the use of LFR is clearly set out, communicated and understood then it should be easier to judge whether or not the deployment was necessary in a democratic society and whether the operation has been a success. It should therefore be more straightforward to identify relevant and meaningful performance metrics.

2. The Watchlist

6.17. The size (number), diversity, lawful basis upon which images are used (including those later added and subtracted during an operation) and the intended purpose of the watchlist are all examples of matters which will be of public interest. The size/content of the watchlist should be determined by the purpose of the deployment. Relating the composition of the watchlist to the purpose, and providing this information to the public are relevant considerations.

3. The Technology – Indications of similarity

6.18. The LFR software does neither confirm or eliminate the identification of a person. When an image is recognised by the technology as being a face, has a likeness to an image which has been programmed in to its watchlist, it provides information to a human decision maker in the form of the two images together with an indication of similarity between them. This similarity score arises from the comparison which the software has made between the images. The effectiveness of this process is relevant as is any variation as to accuracy.

4. The Human Decision Maker

6.19. The human decision maker retains responsibility and accountability for the initial human assessment as to the quality of any indication of likeness and the similarity score provided by the technology. The decision maker will then determine whether or not the indication of likeness is sufficient in their judgement to cause them to reasonably suspect that the images taken from the watch list and that indicated by the technology are so similar as to justify the need for further police action, whether it be to intervene and stop the individual or simply retain the information for 'intelligence purposes'. Decisions which result in the intended outcome against the person sought by the LFR and those which did not, are relevant to a performance framework.

5. Police Intervention and Outcomes

- 6.20. Where police intervention has been directed by a human decision maker, this may in the first instance be to stop and confirm the identity of the subject. The identity of the subject for which the technology had provided a statistical indication of likeness will at this stage either be a confirmed identification made by the police intervention or it will be confirmed that the subject is not the person on the watchlist.
- 6.21. Some example of the nature of information which may be of relevance to the public interest are as follows, (not a definitive list);
- a) The volume of indications of likeness provided by the system in respect of which the human decision maker was satisfied/not satisfied as to likeness of images to the extent that further action was sanctioned.
 - b) The volume of people who were subject to a police intervention where their identity was confirmed as **being** that of an image on a watchlist indicated as a likeness by the technology.
 - c) The volume of people who were subject to a police intervention where their identity was confirmed as **not being** that of an image on a watchlist indicated as a likeness by the technology.
 - d) The number/proportion of people who were on a watchlist and were subject to police action which met the purpose for which they were included on it.
 - e) Appropriate diversity information which is relevant to the public interest in respect of the above.
- 6.22. In balancing the importance of transparency and confidentiality in the public interest, the nature of the performance information and the extent of the detail provided to the public, are matters of judgement for the police in consideration of a number of factors, including the circumstances and context in which the technology is operated.

7. Accountability and Certification

Accountability

- 7.1. The police are accountable for the legitimacy, integrity and efficiency of the services they provide to their communities. There is an established and comprehensive framework of accountability mechanisms which hold the performance of the police service, and the performance of individual police officers to account. They do not require repeating in this document.
- 7.2. In the context of communities, the more consultative the police are the more accountable they become. The Police and Crime Commissioner has a particularly important role to play in terms of the governance and accountability of police conduct using LFR.
- 7.3. Police and Crime Commissioners (The Mayor's Office in London) are elected by their communities to be the voice of the people and to hold Chief Constables and the force to account, thereby making the police answerable to the communities they serve.
- 7.4. Under the terms of the Police Reform and Social Responsibility Act 2011, PCCs must:
 - a) secure efficient and effective police for their area;
 - b) appoint the Chief Constable, hold them to account for running the force, and if necessary, dismiss them;
 - c) set the police and crime objectives for their area through a police and crime plan;
 - d) set the force budget and determine the precept;
 - e) contribute to the national and international policing capabilities set out by the Home Secretary; and
 - f) bring together community safety and criminal justice partners, to make sure local priorities are joined up.
 - g) PCCs ensure community needs are met as effectively as possible, and are improving local relationships through building confidence and restoring trust. They work in partnership across a range of agencies at local and national level to ensure there is a unified approach to preventing and reducing crime.
- 7.5. The meaningful engagement of a PCC in the decisions and actions of Chief Constables relevant to the procurement, operation and performance of LFR should be assured, as a key ingredient of the accountability for police conduct. More information regarding the role of the PCC can be accessed at the below link;

<https://www.apccs.police.uk>

- 7.6. The purpose of Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) is to promote improvements in policing (and fire & rescue services) to make everyone safer. The inspection and assessment activities which they undertake holds police performance to account and promulgates learning and improvement.

<https://www.justiceinspectors.gov.uk/hmicfrs/>

Certification

- 7.7. The office of the Surveillance Camera Commissioner in conjunction with three UKAS (United Kingdom Accreditation Service) accredited certification bodies has developed a two-step certification process. Organisations that successfully achieve certification are awarded a certificate of compliance by the Surveillance Camera Commissioner and are able to use the Commissioner's certification mark on their website and other communications to indicate they comply with the SC Code.
- 7.8. Certification is a means whereby an organisation can reassure the public that their operation of a surveillance camera system has been independently assessed and certified to industry and regulatory standards as being operated in a manner which complies with the Surveillance Camera Code of Practice.
- 7.9. Further detail of the SCC Certification Scheme is accessible at the below link.

<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-third-party-certification-scheme>

Annex A – Summary List of Recommendations

Paragraph 2.17 – The SCC recommends that the Home Office consult with others including the National Police Chief’s Council and the Association of Police and Crime Commissioners to establish;

- a) a national procurement strategy which provides the right tools and engenders public confidence;
- b) a means by which the credentials of LFR technology can be suitably analysed and assessed so as to determine risks associated with matters such as accuracy, similarity thresholds, human decision making (amongst others);
- c) national standards (e.g. privacy/security by design/default) to help to inform future procurement, equipment employment and deployment decision making as well as better enabling the police to comply with the Public Sector Equality Duty (PSED) and other statutory and risk assessment obligations in respect of their use of LFR.

Paragraph 2.26 – The SCC recommends that where police forces are considering operating LFR they should develop mechanisms which provide for meaningful and independent ‘ethical oversight’ of their decision making and operational conduct. Such considerations should be applied as part of the initial police planning processes and be established before any operational activity commences. Ethics Committees, where they exist, may meaningfully be consulted in the first instance and any relevant oversight arrangements determined. Where there is no digital or ethics committee structure within a police force region there may be local multi agency structures which could play such a role, similar to those which exist in scrutinising police stop and search activities. Such matters are for Chief Officers and their Police and Crime Commissioners to consider where relevant. The SCC is supportive in particular of including the police use of LFR within the ambit of decision making which should be covered under the establishment of a national Digital and Data Ethics Committee by APCC and NPCC.

Paragraph 3.86 – The SCC recommends that the Home Office, regulators and other stakeholders collaborate to consider the development of a single ‘integrated impact assessment’ process/format which provides for a comprehensive approach to such matters. This is to improve focus, reduce duplication, reduce bureaucracy and avoid gaps whilst fulfilling statutory and organisational requirements in so far as they relate to the use of biometric and other surveillance enhancing technologies as part of a surveillance camera system including, but not exclusive to LFR.

Paragraph 3.91 – The SCC recommends as good practice, that when procuring LFR systems an assessment is made as to whether the software or hardware which is to be procured and is to be used, has a known vulnerability, or history/pedigree of vulnerability to being ‘hacked’. Firewalls, anti-virus and other risk mitigation measures should be addressed particularly if the system is to be networked or cloud storage considered. Standalone systems are not immune from cyber vulnerability particularly if ‘pen drive’ or other image/data transfer media are to be permitted. Operational

disciplines should ensure that processes are appropriately cognisant of cyber risks and staff using the system should be aware of those risks and how to mitigate them.

Paragraph 4.15 – The SCC recommends that the Home Office and Government review the laws which govern the conduct of overt surveillance by the police where such surveillance conduct employs biometric or similarly intrusive technology.

Paragraph 4.16 – The SCC recommends that in consideration of the observations of the Court of Appeal in the Bridges case at Paragraph 118 of that judgement, that the Home Office and Secretary of State honour the commitment made in the Home Office Biometrics Strategy ('Better Public Services Maintaining Public Trust' (Chapter 3 page 13)) which was published in June 2018 to review and update the Surveillance Camera Code of Practice in collaboration with the Surveillance Camera Commissioner so as to take cognisance of the evolving nature of public space overt surveillance by agents of the state since its introduction in June 2013, including – but not exclusive to – the challenges presented by the use of technology.

Paragraph 4.17 – In both of the above cases, the SCC recommends in particular that clear provision is made for ethical standards, equality, legality and the governance and accountability of operational and intrusive conduct.

Paragraph 4.18 – The SCC recommends that the NPCC and the Home Office consider developing consistent approval and decision making structures which approves operational police conduct overtly using LFR and which takes in to account and coordinates the breadth of statutory, regulatory and organisational roles and responsibilities which are inherent in the police use of LFR. Such arrangements should include considerations which are applicable to watchlists, system probability thresholds, the specific parameters of approved operational deployments of LFR (including any subsequent changes) and processes of review. In particular the SCC recommends that the strategic and operational decision making should be made by an officer of an appropriately senior rank who is not engaged in the day to day direction of the operation in connection with which LFR is to be operated (similar to that which exists in the statutory context of RIPA where an authorising officer performs such a role), so as to demonstrate a higher degree of transparency, integrity and operational independence in such matters.

Paragraph 4.65 – In recognising the quality of their work in respect of digital ethics, the SCC recommends that the College of Policing and the NPCC consider whether at a national level, the role of the human decision maker should be better defined, “structured” within a surveillance camera system, benefit from further nationally produced guidance or training and the role quality assured by means of meaningful analysis of performance. Such standards where they are established should be consistent across different police forces/organisations and for Chief Officers to have regard. In any event it is good practice for there to be measures in place which quality assure and demonstrate the performance of human decision making associated with LFR. This information may be made publicly available as appropriate.

Paragraph 6.10 – The SCC considers that it would be beneficial for the NPCC to develop a meaningful and national suite of relevant performance indicators which demonstrates as a minimum, the purpose, successes, failures, outcomes, the nature and extent of intrusion and the accuracy and diversity of impact of their LFR operations. The SCC recommends that such a body of performance information should be developed in a manner which is nationally consistent amongst police forces in England and Wales and recommends that HMICFRS are appropriately consulted on such matters.

Paragraph 6.11 – The SCC further recommends that the police should develop nationally consistent terminology attributable to the use of LFR systems. In doing so more meaningful analysis, comparison, understanding and learning may be derived by the police, the public and the wider stakeholder community.

Annex B – Guiding Principles of SC Code

The SC Code provides 12 guiding principles which should be adopted by system operators. They are as follows:

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.

Annex C – Forensic Science Regulators approach to validation

The validation of any forensic science method being introduced into the Criminal Justice System should follow the risk-based approach based on the Forensic Science Regulator’s Codes of Practice and Conduct prior to deployment.

The Forensic Science Regulator has issued general guidance of validation, although workflows focus on traditional forensic science applications. The Government Office for Science report “Forensic science and beyond: authenticity, provenance and assurance – evidence and case studies”¹ incorporated Forensic Science Regulator’s approach to illustrate the path for innovation to market and this has been further developed here to also include Data Protection Impact Assessments (DPIA).

¹ Available from: (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/506462/gs-15-37b-forensic-science-beyond-evidence.pdf – page 38, figure 1).

