SURVEILLANCE CAMERA COMMISSIONER

The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems

Section 33 Protection of Freedoms Act 2012

Published: March 2019

1. Introduction

1.1 The use of automated facial recognition technology is becoming a technological ingredient of our digitally enhanced society. Such systems are increasingly in everyday use for our convenience and a growing feature of the surveillance and other IT systems being used and operated by private and retail sectors. Within this context there is a propensity for police, law enforcement agencies and other public bodies to consider making use of these technologies in pursuit of their public duties. It is acknowledged that the use of new technologies when integrated with surveillance camera systems can bring added benefits to the police in protecting the public. Those same technologies however have significant capabilities to intrude upon the right to privacy, the freedom of assembly and association, the freedom of expression and other fundamental freedoms, of citizens and the protection from discrimination in respect of those rights and freedoms. If not lawfully, responsibly and ethically operated this technology may adversely impact upon the public confidence which the police would seek to engender by their use in the first place.

1.2 Chief Officers of Police and Police and Crime Commissioners in England and Wales are amongst a suite of 'relevant authorities' as defined by the Protection of Freedoms Act 2012 and as such have additional statutory responsibilities when operating surveillance camera systems in public places.

1.3 This guidance is produced by the Surveillance Camera Commissioner (the SCC) to assist 'relevant authorities' to comply with their statutory obligations arising from Section 31(1) Protection of Freedoms Act 2012 (PoFA) and the Surveillance Camera Code of Practice (SC Code) when overtly operating surveillance camera systems in public places in England and Wales, including those which make use of face recognition technology.

1.4 Nothing within this guidance replaces any of the content of the SC Code, which should be read and considered alongside this supplementary *and additional* guidance.

1.5 For the purpose of this guidance the term 'Automated Facial Recognition' (AFR) will be used throughout to describe technology which is used in connection with or otherwise integrated with an overt surveillance camera system operating in public places in England and Wales. References within this document to a 'surveillance camera system' should be similarly construed.

1.6 Although this guidance is primarily aimed at 'relevant authorities' as defined at Section 33(5) PoFA, the SCC encourages other operators of surveillance camera systems who are not bound by any duty to have regard to the SC Code, to voluntarily adopt its guiding principles in accordance with paragraph 1.17. In that regard this guidance is similarly provided for any value it may have to those operators.

1.7 The SCC provides this advice by virtue 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'

1.8 The information and guidance provided within this document are the views of the SCC, who is not a judicial authority, and simply indicates the way in which the Commissioner is minded to construe the particular statutory provisions arising from PoFA and those provisions within the SC Code in the absence of case law.

1.9 The SCC has no powers of inspection, audit or compliance and his role is simply advisory. The SCC does not give legal advice and nothing within this document should be construed or otherwise interpreted as amounting to such. Relevant authorities are encouraged to seek their own legal guidance in respect of any matter within this guidance as they consider to be appropriate.

1.10 This document is to be properly promoted by relevant authorities and Senior Responsible Officers (SRO) appointed by them to ensure compliance with Section 33 PoFA and the SC Code. It is also made available to the general public to demonstrate transparency of regulatory approach.

1.11 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)

1.12 The Surveillance Camera Commissioner's office can be contacted at: scc@sccommissioner.gsi.gov.uk.

2. Human Rights

2.1 The Human Rights Act 1998 sets out the fundamental rights, freedoms and protections that citizens within the UK are entitled to from intrusion by the state as enshrined within the ECHR. In the context of the overt operation of surveillance camera systems in public places, Article 8 (respect for private and family life) is a fundamental consideration for system operators to address.

2.2 However, the use of AFR and similar technologies in crowded places and selected sites will significantly enhance the capabilities of a surveillance camera system to intrude and gather private information of a citizen. They is also potential for impacts on other human rights including:

- 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

2.3 This is not to say that every deployment of AFR automatically affects those rights, or will result in violations. However, an assessment of potential harm and impact should be a fundamental consideration of each and every intended deployment of AFR before any such deployment of the technology is made. An assessment of risk and risk management measures including an assessment of intended and collateral intrusion should be

undertaken and appropriately documented by the relevant authority. It is best practice, where possible, to make risk assessments publically available, for example by publishing them on your website.

3. Legal Framework

3.1 In the first instance a relevant authority should be clear and transparent as to the legal basis upon which they seek to rely to justify the use of AFR. A legal framework exists which lends itself to the operation of surveillance camera systems; primarily (but not exclusively) they include Protection of Freedoms Act 2012, Regulation of Investigatory Powers Act 2000 and Data Protection Act 2018. **Operators of surveillance camera systems which make use of face recognition technology are advised to seek advice from their legal advisers in respect of any matter which arises from their use or intended use of surveillance camera systems which use face recognition technology**.

3.2 The Regulation of Investigatory Powers Act 2000 and the Data Protection Act 2018 are separately regulated by the Investigatory Powers Commissioner's Office (IPCO) and the Information Commissioner's Office (ICO) respectively. Whereas the SC Code signposts those legal responsibilities, operators should familiarise themselves with the relevant legislation and codes of practice before surveillance camera systems making use of face recognition technology are deployed and operated in public.

4. Data Protection

4.1 The Guiding Principles within the SC Code address data protection related considerations which apply when overtly operating surveillance camera systems in public in England and Wales. The Information Commissioner regulates the Data Protection Act 2018 which provides statutory responsibilities for operators and users of surveillance camera systems in respect of the processing and use of personal data obtained by virtue of the use of those systems. Those statutory provisions include a requirement to complete a data protection impact assessment (DPIA). Appropriate guidance as to these matters is provided separately by the ICO. The SCC has developed a DPIA in conjunction with the ICO specifically for organisations in England and Wales that must have regard to the SC Code Section 33(5) of the Protection of Freedoms Act 2012. 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 in accordance with the Data Protection Act 2018. The template is available on the SCC website:

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

4.2 In particular the ICO have issued a code of practice; *'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

5. The Protection of Freedoms Act 2012

5.1 Chapter 1 PoFA addresses '*Regulation of CCTV and Other Surveillance Camera Technology'*. Section 33 of the Act 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'.

5.2 The duty to have regard to the SC Code is addressed later within this guidance. In consideration of Sections 33(3) and 33(4), 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 the Act (PoFA) applies should be disclosed to the Crown Prosecution Service (CPS) whenever such images or other evidence is to be adduced in to judicial proceedings. This 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.

5.3 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).'

5.4 The use of face recognition technology and indeed any other technology which is integrated with the use of a surveillance camera system as defined is therefore capable of falling within the above statutory definition.

6. The Surveillance Camera Code of Practice

6.1 The SC Code is issued by the Secretary of State under section 30 of PoFA and provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities 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

6.2 The SC Code applies to the use of surveillance camera systems by relevant authorities, including those using technologies. It contains a number of provisions which are of specific relevance to the use of face recognition and other technologies integrated with the operation of surveillance camera systems.

6.3 In particular these include the following:

'Used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of legitimate aim and meets a pressing need. (paragraph 2.1)'

'That is not to say that all surveillance camera systems use technology which has a high potential to intrude on the right to respect for private and family life. Yet this code must regulate that potential now and in the future (paragraph 2,3)'

'Any use of facial recognition or other biometric characteristic recognition systems needs to be clearly justified and proportionate in meeting the stated purpose and be suitably validated (Paragraph 3.2.3).

'The Surveillance Camera Commissioner will be a source of advice on validation of such system' (Foot note 4).

6.4 In this context, 'validation' shall include in the end-user requirement that the surveillance camera system 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 by a relevant authority. The validation of any application of an automatic 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 and the general stages are illustrated in Appendix A.

6.5 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. The end-user requirement should include recommendations from regulators (e.g. ICO, SCC) as well as functional requirements such accuracy (e.g. false positive/negative, bias). 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 validation 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 clearly documented.

6.6 The SCC seeks to discharge his responsibilities in that regard by means of early engagement with the relevant police force considering using AFR with their surveillance camera systems, provision of this guidance, prior engagement and discussion with fellow regulators where their particular interests may be engaged (e.g. Information Commissioner's Office, Forensic Science Regulator, Biometrics Commissioner) and consideration of the 'Self-Assessment Tool' completed by the relevant police force (addressed later within this document) which is provided on the SCC website via the following link:

https://www.gov.uk/government/publications/surveillance-camera-code-of-practice-self-assessment-tool

6.7 Additional references within the SC Code which are additionally specific to face recognition systems appear at paragraphs 4.8.1 and 4.12.1.

6.8 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.*

7. The duty to have regard to the SC Code

7.1 *The duty placed upon a relevant authority 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.

7.2 It is important that a relevant authority can demonstrate to an auditable standard that it has applied the principles of the SC Code in respect of the surveillance camera systems it operates, and thereby enable that compliance to be considered and verified in judicial proceedings where necessary, and considered by the public.

7.3 Where a relevant authority has regard for the SC Code yet decides not to adopt any of the provisions contained within it, it should provide detailed and auditable rational for doing so and publish that decision and rationale in the public domain. In such circumstances a relevant authority should consult with its legal advisers beforehand.

8. Regulation of Investigatory Powers Act 2000

8.1 The use of images as part of an AFR system is addressed later in this document. There may be occasions when the inclusion of images on a reference database with the intention of conducting surveillance may be considered as covert surveillance and therefore fall within the bounds of RIPA (SC Code para 4.12.3).

8.2 The intended deployment of AFR as part of a surveillance camera system should be considered by a RIPA Authorising Officer (AO) prior to any deployment taking place so that a decision may be made as to whether an authority should be granted under the provisions of RIPA. Where a RIPA related authorisation is granted by an Authorising Officer thereafter any operational deployment will be managed in accordance with the provisions of that particular legislation.

8.3 Where an Authorising Officer determines that an intended deployment of AFR does not require an authorisation under the provisions of RIPA a record should be made as to that decision together with the underlying rationale.

8.4 Covert surveillance is not regulated by the SC Code or the SCC and further guidance is provided in respect of these matters by the Investigatory Powers Commissioner's Office (IPCO):

https://www.ipco.org.uk/

9. Necessity

9.1 Surveillance camera systems using AFR and 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.

9.2 In essence there must be clarity as to the problem which is to be addressed by the use of AFR and which can be evidenced, and the purpose to which AFR is to be operated. Such purposes may include matters such as the prevention and detection of crime, public safety, national security etc. There should be clarity provided as to why it is considered necessary to use the intrusive capabilities of AFR in such circumstances rather than simply desirable. The availability of AFR capability to address a particular issue is not in itself justification for its use on the grounds of necessity. Just because you can doesn't mean you should. A record should be made as to the case of necessity.

10. Proportionality

10.1 Decisions over the deployment of the most appropriate technology should be proportionate to the stated purpose rather than driven by its availability. In particular the

potential for interference with the ECHR freedoms of citizens should be the fundamental consideration when determining the proportionality of use of AFR against the seriousness of the circumstances and intended outcomes being considered. Any deployment should not be allowed to continue longer than is necessary.

10.2 The potential for intrusion arising from AFR is arguably consistent with 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, (issued pursuant to Section 71 RIPA) should therefore be considered when determining the proportionality of AFR deployment. They are 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.

10.3 A record should be made as to the case of proportionality for the use of AFR. It is best practice, where possible, to make this information publically available, for example by publishing them on your website.

10.4 Proportionality is not only about balancing the effectiveness of AFR 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 aspects of the intended operation of AFR have been fully considered.

11. Risk Assessments

11.1 The use of AFR has the potential to impact upon ECHR rights and thereby influence the sense of trust and confidence within communities. It should be a fundamental consideration of any relevant authority intending to deploy AFR that a detailed risk assessment process is conducted and documented as to the operational risks, community impact risk, privacy and other human rights risks and other risks associated with its use prior to any deployment of the capability is made. Such risks should be considered as part of the decision making processes associated with the necessity and proportionality of its use.

11.2 In particular, in order to give proper consideration to collateral intrusion and other associated risks, a relevant authority must fully understand the capabilities and sensitivity levels of the technical equipment intended to be used, the context of what is sought to be achieved and where and how it is to be deployed. In particular there should be a detailed understanding as to the potential for inaccuracy, error or bias within the technology and a plan documented as to how these matters are to be effectively addressed.

11.3 The AFR technology and algorithms employed are but one ingredient of a 'full system approach' to deployment and regulation of a surveillance camera system. A fundamental requirement of the SC Code and any operational deployment of AFR is that there must be human intervention within final decision making. These systems are devised to alert operators to potential individuals of interest for human operators to review. They are a tool in a process; the overall process requires human intervention and it is this overall process that requires validation. Risk assessment therefore looks at the risks inherent in the technology and how they are mitigated in the overall process; validation assesses the extent to which the mitigation has been successful.

11.4 The risk mitigation plan which sets out how human intervention receives information from the system, assesses its accuracy and makes decisions should be recorded. Such information should be made available to the public. (Public engagement is addressed later in this report).

11.5 When considering the nature and extent of risks associated with the use of AFR integrated with a surveillance camera system, particular regard should be given to risk associated with cyber related considerations. An assessment of cyber related risks to the security of data is of course a requirement of the DPA 2018. However, such an assessment should be broader than assessment of such risks to privacy in the context of processing personal data, and address the broader spectrum of human rights considerations at risk of being infringed by the technology together with other operational and contextual risks. For example an assessment should be made as to whether the software or hardware in use has a vulnerability, or history 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 particular 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. These matters should be documented as part of a broader risk assessment approach.

12. Self Assessment Tools

12.1 There is an expectation placed upon a relevant authority that it is transparent regarding its duty to have regard for the SC Code – doing so helps to engender public confidence. This expectation is ever more significant given the enhanced intrusive capabilities associated with the use of AFR and similar technologies. In that regard it is good practice for a relevant authority to complete a Self Assessment Tool (SAT) which is provided by the Surveillance Camera Commissioner. Separate responsibilities and considerations arise from the Data Protection Act 2018 including a requirement to complete a data protection impact assessment (DPIA). Further guidance as to these matters is provided by the ICO (see section 4 above).

12.2 The completion of a SAT is not a statutory requirement of the SC Code. However where a relevant authority does not complete a SAT in respect of a surveillance camera system it should otherwise ensure that it has an audit trail which enables it to sufficiently demonstrate compliance with Section 31(1) PoFA and the SC Code. Furthermore, guiding principle 10 (para 4.10.1) sets out that regular reviews (at least annually) should be carried out to ensure the system remains necessary, proportionate and effective in meeting its stated purpose for deployment. The SAT can be used for such a review.

12.3 A SAT should be completed by a relevant authority for every surveillance camera system operated by them which is relevant to PoFA. A SAT should be kept under review and

updated/refreshed periodically as necessary. Responsibility for undertaking this task must be clearly established by the relevant authority.

12.4 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. Each case must be assessed on its particular merits. In the context of AFR, such systems are in general, more likely to be operated for a defined period of time in support of operational objectives, rather than being operated for more generic monitoring similar to that provided by fixed CCTV systems. AFR should not be deployed any longer than the time 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 addresses the key principles within the SC Code regarding the surveillance camera system that is being operated. If not, or the circumstances or risks associated with such operation change, then a new SAT should be considered.

12.5 As a matter of transparency it is recommended that a SAT should be published in the public domain so that it may be considered by the public and other stakeholders.

13. Governance & Equipment Standards

13.1 It is advisable that decision making by a relevant authority to procure an AFR system in the first instance should engage the Chief Officer of that force. Consideration should be given to any operational and technical standards which have relevance to that system. There are list of standards on the SCC site:

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

13.2 Guiding principle 9 of the SC Code focuses on security measures for surveillance camera systems**.** With more surveillance cameras being linked to the internet this means networks need to be secure by design so cameras are not compromised by cyber attacks and used as a point of entry in to systems and networks. Therefore cyber security measures must be a key consideration when procuring surveillance technologies.

13.3 Decisions to operate AFR by a relevant authority should in the first instance be approved in accordance with instructions provided by the relevant authority unless statutory considerations determine otherwise (e.g. RIPA).

13.4 Where AFR is deployed operationally there should be clear command and control structures in place and clear responsibility and accountability established and documented. Appropriate arrangements must exist to ensure that any deployment of AFR is maintained under continual review so that it is not operated beyond the operational parameters intended (mission creep) or longer than necessary to achieve its intended purpose.

13.5 There should be clear aims and objectives associated with the use of AFR and justifiable timescales provided for deployment.

13.6 Where a system is jointly operated by the police in partnership with other agencies, or the police seek to make use of an AFR system operated by another agency that is not a relevant authority, 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 such cases a documented protocol should be agreed by participating agencies providing clarity as to responsibilities and accountability for statutory compliance.

14. Use of Images

14.1 Where the images of persons are used to form a watch list which is to be used as part of an AFR deployment it is important that the police satisfy themselves that they have legitimacy in retaining those images and also for using them in the manner intended. **This is particularly important in cases where the images intended to be used include those of persons who are not convicted of any offence**. Forces should consider seeking their own legal view on such matters as appropriate.

14.2 Typically watch lists should be created for specific deployments in as narrowly focussed way as practicable. A clear and documented policy should be established to determine and justify the inclusion of individuals on a watch list to be used as part of an AFR system (SC Code para 4.12.2).

14.3 Images added to watch lists should not be retained for longer than is necessary to fulfil the purpose for which they were originally added to the list – for example the deployment of AFR at a specific event. The safe guarding of the images used to form a watch list is the responsibility of the implementing authority, the risk assessment should have identified the key issues. The policy or procedure on 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).

15. Ethical Principles

15.1 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 Governing Principles should be demonstrably applied by a relevant authority operating AFR. 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.

15.2 Further details as to these issues can be found 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

16. Data Integrity

16.1 It is important that there are effective safeguards in place to ensure data integrity of recorded information and its usefulness for the purpose for which it is intended.

16.2 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 accessible by means of the following link:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/651966/100_-_2017_10_09_-_The_Codes_of_Practice_and_Conduct_-_Issue_4_final_web_web_pdf__2_.pdf

17. Public Engagement

17.1 Transparency and accountability on the part of a relevant authority are key elements of public interest when operating AFR in public places. Not only are these legislative requirements, they are essential contributing factors to engendering public trust and confidence in the operation of surveillance camera systems.

17.2 The ICO provides associated guidance in respect of these matters to ensure that the responsibilities of the Data Protection Act 2018 are discharged by system operators.

17.3 People in public places should be aware whenever they are being monitored by a surveillance camera system and the provision of information is the first step and a key mechanism of accountability. If they are not made aware this may be considered as covert surveillance and therefore fall within the bounds of RIPA (see section 8 of this document).

17.4 Relevant authorities should ensure that they have effective mechanisms for consultation and engagement with the public and partners. Effective engagement should be meaningful and a continuum before and after AFR operations. In particular engagement with representatives of those affected by any intended use of AFR and those communities which may feel disproportionally affected is essential. A relevant authority should be proactive in publishing information which should include publishing successes and failures.

18. Staged approach to deployment

18.1 The SCC has developed a ‘passport to compliance’ document which sets out a staged approach to which is necessary when planning, implementing and operating a surveillance camera system to ensure it complies with the SC Code:

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

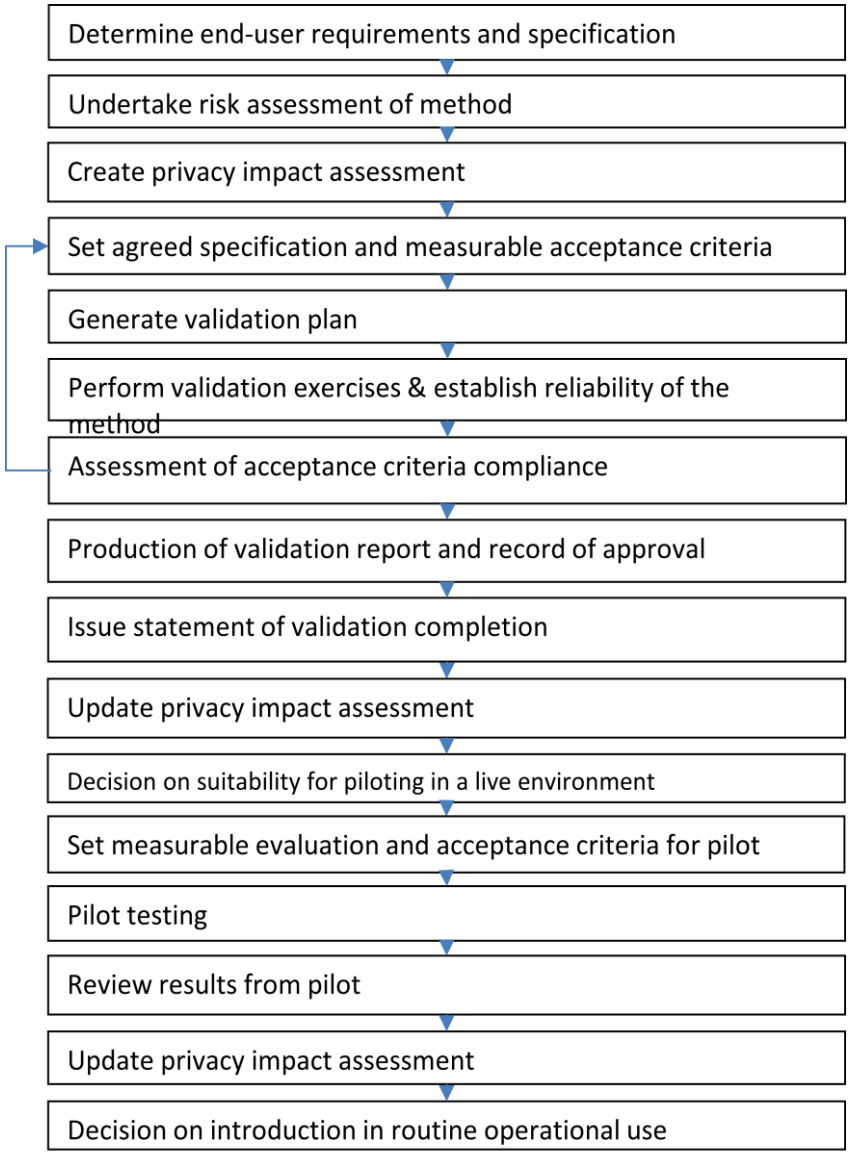
18.2 The Forensic Science Regulator has also developed a flowchart which sets out each stage of a process that should be followed when piloting automatic facial recognition – see Appendix A

Appendix A

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).