Home Office

Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012

Introduction

Definitions

1.1 In this code:

- "1998 Act" means the Data Protection Act 1998.
- "2000 Act" means the Regulation of Investigatory Powers Act 2000.
- "2012 Act" means the Protection of Freedoms Act 2012.
- "Overt surveillance" means any use of surveillance for which authority does not fall under the 2000 Act.
- "Public place" has the meaning given Section 16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.
- "Relevant authority" has the meaning given by Section 33(5) of the 2012 Act.
- "Surveillance camera systems" has the meaning given by Section 29(6) of the 2012 Act and is taken to include: (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 the images or information obtained by (a) or (b); (d) any other systems associated with, or otherwise connected with (a), (b) or (c)[1].
- "System Operator" - person or persons that take a decision to deploy a surveillance camera system, and/or are responsible for defining its purpose, and/or are responsible for the control of the use or processing of images or other information obtained by virtue of such system.
- "System User" – person or persons who may be employed or contracted by the system operator who have access to live or recorded images or other information obtained by virtue of such system.

[1] Excludes any camera system with relevant type approval of a prescribed device under Section 20 of the Road Traffic Offenders Act 1988 used exclusively for enforcement purposes, which captures and retains an image only when the relevant offence is detected and with no capability to be used for any surveillance purpose. For example, for the enforcement of speeding offences.

Background

1.2 This code of practice is issued by the Secretary of State under Section 30 of the 2012 Act. It provides guidance on the appropriate and effective use of surveillance camera systems by relevant authorities (as defined by section 33 of the 2012 Act) in England and Wales who must have regard to the code when exercising any functions to which the code relates. Other operators and users of surveillance camera systems in England and Wales are encouraged to adopt the code voluntarily. It is a significant step in the ongoing process of delivering the government's commitment to the 'further regulation of CCTV' which it believes is a task that is best managed in gradual and incremental stages. As understanding and application of the code increases the government may consider including other bodies as relevant authorities who will have to have regard to the code.

Purpose of the code

1.3 Surveillance camera systems are deployed extensively within England and Wales, and these systems form part of a complex landscape of ownership and operation. Where used appropriately, these systems are valuable tools which contribute to public safety and security and in protecting both people and property.

1.4 The government is fully supportive of the use of overt surveillance cameras in a public place whenever that use is: in pursuit of a legitimate aim; necessary to meet a pressing need[2]; proportionate; effective, and; compliant with any relevant legal obligations.

1.5 The purpose of the code will be to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them. The government considers that wherever overt surveillance in public places is in pursuit of a legitimate aim and meets a pressing need, any such surveillance should be characterised as surveillance by consent, and such consent on the part of the community must be informed consent and not assumed by a system operator. Surveillance by consent should be regarded as analogous to policing by consent. In the British model of policing, police officers are citizens in uniform. They exercise their powers to police their fellow citizens with the implicit consent of their fellow citizens. Policing by consent is the phrase used to describe this. It denotes that the legitimacy of policing in the eyes of the public is based upon a general consensus of support that follows from transparency about their powers, demonstrating integrity in exercising those powers and their accountability for doing so.

2 A public authority will be bound by the Human Rights Act 1998 and will therefore be required to demonstrate a pressing need when undertaking surveillance as this may interfere with the qualified right to respect for private and family life provided under Article 8 of the European Charter of Human Rights. This is the case whether or not that public authority is a relevant authority. A system operator who is not a public authority should nevertheless satisfy themselves that any surveillance is necessary and proportionate.

1.6 In order to achieve this, the code sets out guiding principles that should apply to all surveillance camera systems in public places. These guiding principles are designed to provide a framework for operators and users of surveillance camera systems so that there is proportionality and transparency in their use of surveillance, and systems are capable of providing good quality images and other information which are fit for purpose.

1.7 To support the practical application of these guiding principles by a system operator, the Surveillance Camera Commissioner will provide information and advice on appropriate and approved operational and technical standards for various aspects of surveillance camera systems and on appropriate and approved occupational and competency standards for persons using these systems or processing images and information obtained by these systems to supplement this code.

1.8 This code has been developed to address concerns over the potential for abuse or misuse of surveillance by the state in public places, with the activities of local authorities and the police the initial focus of regulation. However, the government fully recognises that many surveillance camera systems within public places are operated by the private sector, by the third sector or by other public authorities (for example, shops and shopping centres, sports grounds and other sports venues, schools, transport systems and hospitals). Informed by advice from the Surveillance Camera Commissioner, the government will keep the code under review and may in due course consider adding others to the list of relevant authorities pursuant to section 33(5)(k) of the 2012 Act.

Scope of surveillance activity to which this code applies

1.9 The code applies to the use of surveillance camera systems that operate in public places in England and Wales, regardless of whether or not there is any live viewing, or recording of images or information or associated data.

1.10 Covert surveillance by public authorities (as defined in Part II of the 2000 Act) is not covered by this code but is regulated by the 2000 Act. Covert surveillance in public places by those who do not fall within the 2000 Act (for example, the private operator of a surveillance camera system in a shopping centre) may be used as part of a specific investigation in exceptional and justifiable circumstances. Any such covert use of private systems by or on behalf of a public authority (with the authority's knowledge) immediately places such use within the bounds of the 2000 Act.

Effect of the Code

1.11 A relevant authority must follow a duty to have regard to the guidance in this code when, in exercising any of its functions, it considers that the future deployment or continued deployment of surveillance camera systems to observe public places may be appropriate. This can include the operation or use of any surveillance camera systems, or the use or processing of images or other information obtained by virtue of such systems. The duty to have regard to this code also applies when a relevant authority uses a third party to discharge relevant functions covered by this code and where it enters into partnership arrangements. Contractual provisions with such third party service providers or partners should ensure that contractors are obliged by the terms of the contract to have regard to the code when exercising functions to which the code relates. The duty to have regard does not extend to such third party service providers or partners unless they themselves are a relevant authority.

1.12 A failure on the part of any person to act in accordance with any provision of this code does not of itself make that person liable to criminal or civil proceedings. This code is, however, admissible in evidence in criminal or civil proceedings, and a court or tribunal may take into account a failure by a relevant authority to have regard to the code in determining a question in any such proceedings.

1.13 Other operators of surveillance camera systems who are not defined as relevant authorities are encouraged to adopt this code and its guiding principles voluntarily. Such system operators are not, however, bound by any duty to have regard to this code.

Relevant documents

1.14 The Information Commissioner's CCTV Code of Practice provides good practice guidance for those involved in operating CCTV and other surveillance camera systems which view or record images of individuals including information derived from those images that may be related to them such as a vehicle registration mark. Its primary purpose is to help those involved in such activities to comply with their legal obligations under the 1998 Act.

1.15 The Covert Surveillance and Property Interference Revised Code of Practice published by the Home Office provides guidance on the use of covert surveillance by public authorities under the 2000 Act. Further guidance on the application of the 2000 Act is available from the Office of the Surveillance Commissioners.

1.16 This code provides guidance on the use of surveillance camera systems but does not replace or remove any statutory obligations on operators or users of such systems to comply with the provisions of both the 1998 Act and the 2000 Act.

Chapter 2

Overview and Guiding Principles

2.1 Modern and forever advancing surveillance camera technology provides increasing potential for the gathering and use of images and associated information. These advances vastly increase the ability and capacity to capture, store, share and analyse images and information. This technology can be a valuable tool in the management of public safety and security, in the protection of people and property, in the prevention and investigation of crime, and in bringing crimes to justice. Technological advances can also provide greater opportunity to safeguard privacy. Used appropriately, current and future technology can and will provide a proportionate and effective solution where surveillance is in pursuit of a legitimate aim and meets a pressing need.

2.2 In general, any increase in the capability of surveillance camera system technology also has the potential to increase the likelihood of intrusion into an individual's privacy. The Human Rights Act 1998 gives effect in UK law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, such as the prohibition on torture, whilst others are qualified, meaning that it is permissible for the state to interfere with those rights if certain conditions are satisfied. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by Article 8 of the ECHR[3].

2.3 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. In considering the potential to infringe upon privacy, it is important to take account of the fact that expectations of privacy are both varying and subjective. In general terms, one of the variables is situational, and in a public place there is a zone of interaction with others which may fall within the scope of private life. An individual can expect to be the subject of surveillance in a public place as CCTV, for example, is a familiar feature in places that the public frequent. An individual can, however, rightly expect surveillance in public places to be both necessary and proportionate, with appropriate safeguards in place.

3 Article 8 of the European Charter on Human Rights reads as follows:
Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

2.4 The decision to use any surveillance camera technology must, therefore, be consistent with a legitimate aim and a pressing need. Such a legitimate aim and pressing need must be articulated clearly and documented as the stated purpose for any deployment. The technical design solution for such a deployment should be proportionate to the stated purpose rather than driven by the availability of funding or technological innovation. Decisions over the most appropriate technology should always take into account its potential to meet the stated purpose without undue intrusion upon the right to privacy and family life. Furthermore, any deployment should not continue for longer than necessary.

2.5 The starting point for a system operator in achieving the most appropriate balance between public protection and individual privacy and thereby achieving overt surveillance by consent is to adopt a single set of guiding principles that are applicable to all surveillance camera systems in public places. Following these guiding principles allows a system operator to establish a clear rationale for any overt surveillance camera deployment in public places, to run any such system effectively, helps ensure compliance with other legal duties and to maximise the likelihood of achieving surveillance by consent.

Guiding Principles

2.6 System operators should adopt the following 12 guiding principles:

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 its purpose has 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 a pressing need, 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 matches against a reference database for matching purposes should be accurate and kept up to date.

The Development or use of Surveillance Camera Systems

This chapter expands on guiding principles 1-4 which address the development or use of surveillance camera systems

Principle 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.

3.1.1 Surveillance camera systems operating in public places must always have a clearly defined purpose (or purposes) in pursuit of a legitimate aim and necessary to address a pressing need. Such a legitimate aim and pressing need might include national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. That purpose should be capable of translation into clearly articulated objectives against which the ongoing requirement for operation or use of the systems and any images or other information obtained can be assessed.

3.1.2 In assessing whether a system will meet its objectives, and in designing the appropriate technological solution to do so, a system operator should always consider the requirements of the end user of the images, particularly where the objective can be characterised as the prevention, detection and investigation of crime and the end user is likely to the police and the criminal justice system.

3.1.3 A surveillance camera system should only be used in a public place for the specific purpose or purposes it was established to address. It should not be used for other purposes that would not have justified its establishment in the first place. Any proposed extension to the purposes for which a system was established and images and information are collected should be subject to consultation before any decision is taken.

Principle 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.

3.2.1 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. Deploying surveillance camera systems in public places where there is a particularly high expectation of privacy, such as toilets or changing rooms, should only be done to address a particularly serious problem that cannot be addressed by less intrusive means. Such deployment should be subject to regular review to ensure it remains necessary.

3.2.2 Any proposed deployment that includes audio recording in a public place is likely to require a strong justification of necessity to establish its proportionality. There is a strong presumption that a surveillance camera system must not be used to record conversations as this is highly intrusive and unlikely to be justified.

3.2.3 Any use of facial recognition or other biometric characteristic recognition systems needs to clearly justified and proportionate in meeting the stated purpose, and be suitably validated[4]. It should always involve human intervention before decisions are taken that affect an individual.

3.2.4 This principle points to the need for a privacy impact assessment process to be undertaken whenever the development or review of a surveillance camera system is being considered to ensure that the purpose of the system is and remains justifiable, there is consultation with those most likely to be affected, and the impact on their privacy is assessed and any appropriate safeguards can be put in place. Where such an assessment follows a formal and documented process, such processes help to ensure that sound decisions are reached on implementation and on any necessary measures to safeguard against disproportionate interference with privacy. This also demonstrates that both the necessity and extent of any interference with Article 8 rights has been considered.

3.2.5 A privacy impact assessment also helps assure compliance with obligations under the 1998 Act. Comprehensive guidance, the Privacy Impact Assessment handbook, is available through the Information Commissioner's Office. This encourages organisations to devise and implement an assessment process that is appropriate and proportionate to their circumstances.

Principle 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.

3.3.1 People in public places should normally be made aware whenever they are being monitored by a surveillance camera system, who is undertaking the activity and the purpose for which that information is to be used. This is an integral part of overt surveillance and is already a legal obligation under the 1998 Act. Furthermore, such awareness on the part of the public supports and informs the concept of surveillance by consent.

3.3.2 Surveillance by consent is dependent upon transparency and accountability on the part of a system operator. The provision of information is the first step in transparency, and is also a key mechanism of accountability. In the development or review of any surveillance camera system, proportionate consultation and engagement with the public and partners (including the police) will be an important part of assessing whether there is a legitimate aim and a pressing need and whether the system itself is a proportionate response. Such consultation and engagement also provides an opportunity to identify any concerns and modify the proposition to strike the most appropriate balance between public protection and individual privacy.

4 The Surveillance Camera Commissioner will be a source of advice on validation of such systems.

3.3.3 This means ensuring effective engagement with representatives of those affected and in particular where the measure may have a disproportionate impact on a particular community. It is important that consultation is meaningful and undertaken at a stage when there is a realistic prospect of influencing developments.

3.3.4 System operators should be proactive in the provision of regularly published information about the purpose, operation and effect of a system. This is consistent with the government's commitment to greater transparency on the part of public bodies.

3.3.5 In addition to the proactive publication of information about the stated purpose of a surveillance camera system, good practice includes considering the publication of information on the procedures and safeguards in place, impact assessments undertaken, performance statistics and other management information and any reviews or audits undertaken. Public authorities should consider including this information as part of their publication schemes under the Freedom of Information Act 2000.

3.3.6 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.

3.3.7 A system operator should have an effective procedure for handling concerns and complaints from individuals and organisations about the use of surveillance camera systems. Information about complaints procedures should be made readily available to the public. Where a complaint is made and the complainant not satisfied with the response there should be an internal review mechanism in place using a person not involved in handling the initial complaint. Complaints must be handled in a timely fashion and complainants given an indication of how long a complaint may take to handle at the outset.

3.3.8 Once a complaint has been concluded information should be provided to the complainant about any regulatory bodies who may have jurisdiction in that case such as the Information Commissioner or the Investigatory Powers Tribunal.

3.3.9 Where a complaint or other information comes to the attention of a relevant authority or other system operator that indicates criminal offences may have been committed in relation to a surveillance camera system then these matters should be referred to the appropriate body, such as the police or the Information Commissioner for any offences under the 1998 Act.

3.3.10 In line with government commitment towards greater transparency on the part of public authorities a system operator should publish statistical information about the number and nature of complaints received and how these have been resolved on an annual basis at least.

3.3.11 The government's further commitment to 'open data' means that public authorities should consider making information available in reusable form so others can develop services based on this data. This would extend to information about surveillance camera systems.

3.3.12 The Surveillance Camera Commissioner has no statutory role in relation to the investigation and resolution of complaints. System operators should, however, be prepared to share information about the nature of complaints with the Surveillance Camera Commissioner on an ad hoc basis to assist in any review of the operation of this code of practice.

Principle 4 - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

3.4.1 Persons considering the need to develop a surveillance camera system should give due consideration to the establishment of proper governance arrangements. There must be clear responsibility and accountability for such a system. It is good practice to have a designated individual responsible for the development and operation of a surveillance camera system, for ensuring there is appropriate consultation and transparency over its purpose, deployment and for reviewing how effectively it meets it purpose.

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

3.4.3 A surveillance camera system may be used for more than one purpose. For example, one purpose might be crime prevention and detection, and another traffic management. Accountability for each purpose may rest within different elements of a system operator's management structure. Should that be the case, then it is good practice for the governance arrangements to include those accountable for each purpose and facilitate effective joint working, review and audit, decision making and public engagement.

The use or processing of images or other information obtained by virtue of such systems

This chapter expands on guiding principles 5-12 which address the use or processing of images and information.

Principle 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.

4.5.1 There are significant benefits in having clear policies and procedures for the operation of any surveillance. This can not only aid the effective management and use of a surveillance camera system but also help ensure that any legal obligations affecting the use of such a system are addressed.

4.5.2 A surveillance camera system operator is encouraged to follow a quality management system as a major step forward in controlling and improving their key processes. Where this is done through certification against a quality management standard it can provide a robust operating environment with the additional benefit of reassurance for the public that the system is operated responsibly and effectively, and the likelihood of any breech of individual privacy is greatly reduced.

4.5.3 It is good practice that the communication of rules, policies and procedures should be done as part of the induction and ongoing professional training and development of all system users. This should maximise the likelihood of compliance by ensuring system users are competent, have relevant skills and training on the operational, technical and privacy considerations and fully understand the policies and procedures. It is requirement of the 1998 Act that organisations ensure the reliability of staff having access to personal data, including images and information obtained by surveillance camera systems.

4.5.4 Wherever there are occupational standards available which are relevant to the roles and responsibilities of their system users, a systems operator should consider the benefits and any statutory requirements associated with such occupational standards. The Surveillance Camera Commissioner will provide advice and guidance on relevant occupational competency standards.

4.5.5 Wherever a surveillance camera system covers public space a system operator should be aware of the statutory licensing requirements of the Private Security Industry Act 2001. Under these requirements, the Security Industry Authority (SIA) is charged with licensing individuals working in specific sectors of the private security industry. A public space surveillance (CCTV) licence is required when operatives are supplied under a contract for services. It is a criminal offence for staff to be contracted as public space surveillance CCTV operators in England, Wales, Scotland or Northern Ireland without an SIA licence.

4.5.6 SIA licensing is dependent upon evidence that an individual is fit and proper to fulfil the role, and evidence of their ability to fulfil a role effectively and safely with the right skills and knowledge. There are various relevant qualifications available, and training to attain these is delivered by a range of different accredited providers.

4.5.7 Even where there is no statutory licensing requirement, it is good practice for a system operator to ensure that all staff who either manage or use a surveillance camera system, or use or process the images and information obtained by virtue of such systems have the necessary skills and knowledge.

Principle 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 its purpose has been discharged.

4.6.1 Images and information obtained from a surveillance camera system should not be kept for longer than necessary to fulfil the purpose for which it is obtained in the first place. This period should be decided in advance and be the minimum period necessary. This is also a requirement of the 1998 Act and further guidance on this is contained in the ICO CCTV code of practice.

4.6.2 Although images and other information should not be kept for longer than necessary to meet the purposes for recording them, on occasions, a system operator may need to retain images for a longer period, for example where a law enforcement body is investigating a crime to give them the opportunity to view the images as part of an active investigation.

4.6.3 The retention period for different surveillance camera systems will vary due to the purpose for the system and how long images and other information need to be retained so as to serve its intended purpose. It is not, therefore, possible to be prescriptive about maximum or minimum periods. Initial retention periods should be reviewed by a system operator and reset in the light of experience. A proportionate approach should always be used to inform retention periods and these should not be based upon infrequent exceptional cases.

Principle 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.

4.7.1 The disclosure of images and other information obtained from a surveillance camera system must be controlled and consistent with the stated purpose for which the system was established. Disclosure of images or information may be appropriate where the 1998 Act makes exemptions which allow it, or where permitted by other legislation such as the Counter Terrorism Act 2008. These exemptions include where non-disclosure would be likely to prejudice the prevention and detection of crime, and for national security purposes. Where a system operator declines a request for disclosure from a law enforcement agency there is provision under Section 9 of and Schedule 1 to the Police and Criminal Evidence Act 1984 to seek a production order from a magistrate.

4.7.2 There may be other limited occasions when disclosure of images to another third party, such as a person whose property has been damaged, may be appropriate. Such requests for images or information should be approached with care, as a wide disclosure may be an unfair intrusion into the privacy of the individuals concerned.

4.7.3 A system operator should have clear polices and guidelines in place to deal with any requests that are received. In particular:

- Arrangements should be in place to restrict disclosure of images in a way consistent with the purpose for establishing the system.
- Where images are disclosed consideration should be given to whether images of individuals need to be obscured to prevent unwarranted identification.
- Those that may handle requests for disclosure should have clear guidance on the circumstances in which disclosure is appropriate.
- The method of disclosing images should be secure to ensure they are only seen by the intended recipient.
- Appropriate records should be maintained.

4.7.4 Judgements about disclosure should be made by a system operator. They have discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once they have disclosed an image to another body, such as the police, then the recipient becomes responsible for their copy of that image. If the recipient is a relevant authority, it is then the recipient's responsibility to have regard to this code of practice and to comply with any other legal obligations such as the 1998 Act in relation to any further disclosures.

4.7.5 Individuals can request images and information about themselves through a subject access request under the 1998 Act. Detailed guidance on this and matters such as when to withhold images of third parties caught in images is included in the ICO CCTV code of practice.

4.7.6 Requests for information from public bodies may be made under the Freedom of Information Act 2000. Detailed guidance on these obligations is included in the ICO CCTV code of practice.

Principle 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.

4.8.1 Approved standards may apply to the system functionality, the installation and the operation and maintenance of a surveillance camera system. These are usually focused on typical CCTV installations, however there may be additional standards applicable where the system has specific advanced capability such as ANPR, video analytics or facial recognition systems, or where there is a specific deployment scenario, for example the use of body-worn video recorders.

4.8.2 Approved standards are available for the operation of surveillance camera systems, including those developed domestically by the British Standards Institute, at a European level by the Comité Européen de Normalisation Électrotechnique[5], or at a global level by the International Electrotechnical Commission. A system operator should consider any approved standards which appear relevant to the effective application of technology to meet the purpose of their system, and taking steps to secure certification against those standards.

4.8.3 Such certification is likely to involve assessment by an independent standards body. This has benefits for a system operator in that the effectiveness of a system is likely to be assured and in demonstrating to the public that suitable standards are in place and being followed.

4.8.4 A current list of recommended standards for consideration by a system operator will be maintained by the Surveillance Camera Commissioner. Such a list will provide detailed guidance on suitable standards and the bodies that are able to accredit performance against such standards.

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

4.9.1 Putting effective security safeguards in place helps ensure the integrity of images and information should they be necessary for use as evidence in legal proceedings. This also helps to foster public confidence in system operators and how they approach the handling of images and information.

4.9.2 Under the 1998 Act, those operating surveillance camera systems or who use or process images and information obtained by such systems must have a clearly defined policy to control how images and information are stored and who has access to them. The use or processing of images and information should be consistent with the purpose for deployment, and images should only be used for the stated purpose for which collected.

4.9.3 Security extends to technical, organisational and physical security and there need to be measures in place to ensure that this is the case and guard against unauthorised use, access or disclosure. The ICO CCTV code of practice gives helpful guidance on achieving this in practice.

[5] CENELEC is also known as the European Committee for Electrotechnical Standardization

Principle 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.

4.10.1 Good practice dictates that a system operator should review the continued use of a surveillance camera system on a regular basis, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose for deployment.

4.10.2 As part of the regular review of the proportionality and effectiveness of a surveillance camera system a system operator should assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

4.10.3 In reviewing the continued use of a surveillance camera system a system operator should consider undertaking an evaluation to enable comparison with alternative interventions with less risk of invading individual privacy, and different models of operation (to establish for example any requirement for 24 hour monitoring). In doing so, there should be consideration of an assessment of the future resource requirements for meeting running costs, including staffing, maintenance and repair.

4.10.4 A system operator should make a summary of such a review available publicly as part of the transparency and accountability for the use and consequences of its operation.

Principle 11 - When the use of a surveillance camera system is in pursuit of a legitimate aim and a pressing need, 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.

4.11.1 The effectiveness of a surveillance camera system will be dependent upon its capability to capture, process, analyse and store images and information at a quality which is suitable for its intended purpose. Wherever the purpose of a system includes crime prevention, detection and investigation, it should be capable, through processes, procedures and training of system users, of delivering images and information that is of evidential value to the criminal justice system. Otherwise, the requirements of the end user of the images, who are likely to be the police and the criminal justice system, will not be able to play their part effectively in meeting the intended purpose of the system.

4.11.2 It is important that there are effective safeguards in place to ensure the forensic integrity of recorded images and information and its usefulness for the purpose for which it is intended to be used. Recorded material should be stored in a way that maintains the integrity of the image and information, with particular importance attached to ensuring that meta data (e.g. time, date and location) is recorded reliably, and compression of data does not reduce its quality. This is to ensure that the rights of individuals recorded by a surveillance camera system are protected and that the material can be used as evidence in court. To do this the medium on which the images and information are stored will be important, and access must be restricted. A record should be kept as an audit trial of how images and information are handled if they are likely to be used as exhibits for the purpose of criminal proceedings in court. Once there is no longer a clearly justifiable reason to retain the recorded images and information, they should be deleted.

4.11.3 It is important that digital images and other related information can similarly be shared with ease with appropriate law enforcement agencies if this is envisaged when establishing a system. If this interoperability cannot be readily achieved it may undermine the purpose for deploying the system.

4.11.4 It is therefore essential that any digital images and information likely to be shared with law enforcement agencies and the criminal justice system are in a data format that is interoperable and can be readily exported, and then stored and analysed without any loss of forensic integrity. In particular:

- A system user should be able to export images and information from a surveillance camera system when requested by a law enforcement agency.
- The export of images and information should be possible without interrupting the operation of the system.
- The exported images and information should be in a format which is interoperable and can be readily accessed and replayed by a law enforcement agency.
- The exported images and information must preserve the quality of the original recording and any associated meta data (e.g. time, date and location).

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

4.12.1 Any use of technologies such as ANPR or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others should not be introduced without regular assessment to ensure the underlying data is fit for purpose.

4.12.2 A system operator should have a clear policy to determine the inclusion of a vehicle registration number or a known individual's details on the reference database associated with such technology. A system operator should ensure that reference data is not retained for longer than necessary to fulfil the purpose for which it was originally added to a database.

4.12.3 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. Further guidance on the application of the 2000 Act is available from the Office of the Surveillance Commissioners.

Surveillance Camera Commissioner

5.1 The Surveillance Camera Commissioner, (the commissioner), is a statutory appointment made by the Home Secretary under Section 34 of the 2012 Act. The commissioner's statutory functions are:

a) encouraging compliance with this code;

b) reviewing the operation of this code; and

c) providing advice about this code (including changes to it or breaches of it).

5.2 In order to fulfil these functions effectively, the commissioner must work closely with other regulators including the Information Commissioner and the Chief Surveillance Commissioner. It is for the commissioner and other regulators to determine how best to maintain these relationships, to agree gateways through which issues flow between the public and the commissioners and how best to publicise and report on arrangements to support these relationships which will be critical in ensuring the success of the code in meeting its purpose.

Ways of working

5.3 The commissioner has no enforcement or inspection powers. In encouraging compliance with the code he should consider how best to ensure that relevant authorities are aware of their duty to have regard for the code and how best to encourage its adoption by other operators of surveillance camera systems.

5.4 The commissioner is expected to provide advice about the relevant operational, technical and occupational competency standards which are available for a system operator to consider in determining how best to meet achieve the purpose of their surveillance whilst meeting legal obligations and making effective use of whilst safeguarding privacy considerations . Such advice can be updated to reflect developments in both the available technology and professional practice.

5.5 In reviewing the operation of the code, the commissioner should consider the impact of regulation against published success criteria and the opportunities to improve compliance in line with better regulation principles.

5.6 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.

5.7 The commissioner may establish an advisory council with specialist sub-groups to support him in fulfilling his functions. Any advisory council or specialist sub-group must have representation from the Home Office and from such persons appearing to the commissioner to be representative of the views of relevant authorities.

5.8 The commissioner must prepare a report about the exercise of his functions during the reporting period, and:

(a) give a copy of the report to the Secretary of State;

(b) the Secretary of State must lay a copy of the report before Parliament; and

(c) the Commissioner must publish the report.

5.9 The reporting periods are set out in the 2012 Act.