Parliamentary Security Camera Policy

Introduction

1) Security cameras are employed in various parts of the Palace of Westminster and its surrounding estate. They are a vital part of the security system for the Palace and make an important contribution to public safety and security by helping to protect both people and the extremely valuable and important heritage and property that are contained within the estate.

2) The use of security camera systems within the parliamentary estate is carefully regulated so that they contribute to the aims for which they are installed and do not become intrusive and a limitation on the freedom or legitimate activities of those visiting or working within Parliament. The purpose of this policy is threefold:

   - to set out the parliamentary policy for the control, use and regulation of surveillance systems within the Palace of Westminster;
   - to ensure that individuals and wider communities are aware of the purposes and general characteristics of the security camera systems that are installed; and
   - to explain the provisions for the use of imagery captured by security camera systems.

3) This policy has been developed using the guidelines laid down in the Home Office Surveillance Camera Code of Practice of June 2013.[1]

4) Security camera systems within Parliament are only used where they are:

   - in pursuit of a legitimate aim
   - necessary to meet a pressing need
   - proportionate
   - effective
   - compliant with any relevant legal obligations.[2]

5) Security camera systems are used in public areas of the parliamentary estate[3] and areas considered vulnerable to intrusion from which the general public are normally

[1] While section 33 of the Protection of Freedoms Act 2012 does not apply to Parliament (and therefore neither does the Code), the parliamentary authorities seek to act, so far as possible, as if it did.

[2] This policy takes into account the guidelines set out in the Home Office Surveillance Camera Code of Practice 2013 as well as relevant provisions of the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Protection of Freedoms Act 2012.

[3] "Public place" has the meaning given by 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.

excluded. Moreover, security camera systems are only deployed where achieving the same effects by other means is not practical or cost effective.[4]

Scope

6) For the purposes of this policy, any reference to the parliamentary estate includes the outbuildings connected with either House as well as the Palace of Westminster and any other spaces which come under the supervision of the Parliamentary authorities. This code applies to the use of overt security camera systems and includes:

- CCTV systems deployed in public areas
- under-vehicle camera systems
- automatic number plate reading systems
- X-ray systems at entry points
- systems for recording or viewing visual images for security purposes
- systems for storing, receiving, transmitting, processing or checking the images or information obtained by the systems above.

System Capabilities

7) The capabilities of the parliamentary security camera systems are subject to development and change. Currently they comprise a network of CCTV cameras covering the internal and external public areas of the parliamentary estate (including the roof, approaches to access points and areas considered vulnerable to intrusion), airport-style baggage scanners at pedestrian entrances, under-vehicle cameras at vehicle entry gates and equipment associated with recording, copying and transmitting images and information derived from the camera systems. The parliamentary authorities also have access to camera imagery from the network of Metropolitan Police Service (MPS) security cameras and traffic cameras in the wider environs of Westminster. Capabilities include staffed monitoring rooms at various points around the Palace of Westminster and its outbuildings and recording equipment capable of capturing the images from all CCTV cameras on the parliamentary estate simultaneously.

[4] For example, by having the same area monitored by a Security Officer.

Provisions for the use of security camera systems

8) The parliamentary security camera systems seek to strike a balance between meeting the need for security and avoiding the possibility of intruding into an individual's privacy. Much of this requires subjective judgement. Policy on the deployment and use of security camera systems is subject to parliamentary scrutiny through the Joint Committee on Security (JCOS) as part of the system for ensuring that appropriate safeguards are in place.

9) The deployment, operation and exploitation of security cameras on the parliamentary estate adhere to the broad provisions set out below. These maintain an appropriate balance between public protection and individual privacy, establish the rationale for the systems, ensure compliance with other legal duties and, by building public confidence, assist in achieving surveillance by consent.

a) The purpose of the security camera systems

The security camera systems operating on the parliamentary estate are deployed primarily to support the security of the Houses of Parliament, prevent unauthorised access to the parliamentary estate or parts thereof and help protect it from attack, protest or disruption by individuals acting maliciously, illegally or outwith the rules and regulations of both Houses. They also have secondary purposes to assist in ensuring public order and safety and to aid the prevention, detection, investigation and prosecution of crime, including damage to property. In this secondary purpose, the ability to record and review footage and images is a necessary part of the capability of the system because the end users are likely to be the police and the criminal justice system. Any proposed extension to the purposes set out above will be subject to consultation with JCOS.

b) Respect for privacy

Security camera systems on the parliamentary estate are only used in areas that can reasonably be regarded as public places or where there is considered to be a particularly high risk of intrusion or vulnerability. They are not used where there is a high expectation of privacy. In addition:

i. Areas under CCTV coverage are routinely reviewed to ensure the capability meets the purposes set out in paragraph 9(a).

ii. Security camera systems do not record conversations.

iii. CCTV is only used for facial or other biometric characteristic recognition when it is clearly justified and proportionate in meeting the stated purpose. Its use for this purpose is subject to approval from the Parliamentary Security

Director, the Serjeant at Arms or Black Rod or their nominated representatives.[5]

iv. When improvements to existing security camera systems are being considered (including replacement of existing ones) or when CCTV monitoring is extended into new areas of the parliamentary estate, a privacy impact assessment is conducted to ensure that the purpose of the system is justifiable. Consultation with those most likely to be affected is also conducted, including through JCOS.

c) Transparency of use

Areas subject to CCTV coverage are clearly signposted. The signs also make it clear why and by whom the area is being monitored. This does not apply to airport-style baggage scanners and under-vehicle camera systems as the nature of the equipment is apparent. Other components of transparency include:

i. Complaints

Any complaint relating to the deployment or operation of the security camera systems should be made within three months of the date on which the complainant became aware of the occurrence complained of. Complaints should initially be addressed to the Serjeant at Arms Directorate in the House of Commons or Black Rod's Department in the House of Lords for informal resolution. Should informal resolution not be possible, then the matter should be made subject to a formal complaint which should be submitted to the Clerk Assistant in the House of Commons or the Reading Clerk in the House of Lords. Once an investigation into the complaint has been completed, a response will be sent to the complainant. This response will include information on other regulatory bodies who may have jurisdiction in the matter such as the Information Commissioner or the Investigatory Powers Tribunal.

ii. Criminal Offences

Should it become apparent, in the course of an investigation, that a criminal offence may have been committed, then the investigator will inform the parliamentary authority under whose supervision the investigation is being conducted and, after consultation with them, refer the matter to an appropriate body such as the Police or the Information Commissioner for any offences under the Data Protection Act 1998.

[5] Nominated representatives are the Deputy Parliamentary Security Director, the Deputy Serjeant at Arms, the Yeoman Usher and the Assistant Serjeant at Arms.

d) Responsibility and accountability for the security camera systems

Ownership of the parliamentary security camera policy and associated regulations is vested jointly in the Clerk of the House and the Clerk of the Parliaments as the Corporate Officers and Data Controllers for the House of Commons and House of Lords respectively.

Oversight of the operation of the security camera systems and the policies, processes and codes of practice governing their use is the responsibility of the Parliamentary Security Director in conjunction with the Serjeant at Arms in the House of Commons and Black Rod in the House of Lords. In implementing this policy, they act as the relevant authorities for the purpose of section 33 of the Protection of Freedoms Act 2012.[6] Within the meaning of the Home Office Surveillance Camera Code of Practice 2013, they also act as the System Operator. As such, they take the decisions to deploy security camera systems, are responsible for defining their purpose and control the use or processing of images or other information obtained from the systems.

Detailed management issues relating to the operation of the security camera systems are addressed on behalf of the System Operator by the Security Systems Steering Group chaired by the Deputy Serjeant at Arms. The Metropolitan Police Service (MPS), as the contracted provider of security to the Houses of Parliament, acts as the System User: the body that is contracted by the System Operator and whose employees have access to live or recorded images or other information obtained from the security camera systems. It is the responsibility of the Parliamentary Security Director, the Serjeant at Arms and Black Rod, or their nominated representatives to ensure that the System User adheres to the parliamentary security camera policy.

e) Policy for the use and operation of the security camera systems

The following conditions apply to the operation and use of the security camera systems:

i. Dedicated system operators are certified by the MPS to operate equipment. Non-certified personnel may also monitor systems on an as required basis for specific purposes; when this happens, they will do so under the overall supervision of a certified operator. In exceptional circumstances such as illness or emergency, non-certified operators may monitor systems; these are logged and the reasons recorded.

[6] "Relevant authority" has the meaning given by Section 33(5) of the Protection of Freedoms Act 2012.

ii. Whilst every effort is made to monitor the system continuously, neither the MPS nor the parliamentary authorities accept liability for any occurrence which is not observed by an operator.

f) Storage of images and information

Images and information derived from the security camera systems is stored to assist in reviewing incidents, to assist in reconstructing events and to enable lessons to be derived. Stored images are also used to facilitate the investigation of public order incidents, criminal acts and breaches of parliamentary rules and regulations. Information from the systems is used, where necessary, for evidential purposes in criminal prosecutions or when dealing with internal disciplinary matters. As a general principle, images are not to be kept for longer than necessary[7] and as a general rule, are usually deleted after 30 days.[8] Exceptions are where:

i. The image or information needs to be retained for evidential purposes;

ii. The information is needed to establish patterns over a longer period of time;

iii. Certain incidents or information is needed for training purposes or to illustrate wider lessons captured on the cameras.

iv. The image or information needs to be retained for the purposes of responding to a data subject access request made under the provisions of the Data Protection Act 1998 or a request made under the Freedom of Information Act 2000.

g) Access to retained images and information

The disclosure of images and other information obtained from the security camera systems is allowed, but release must be consistent with the purposes for which the systems are used and which are set out in paragraph 9(a). Exceptionally, the System Operator will give authority to disclose information to third parties other than the System Operator or System User; for example, to prevent the commission of a crime or apprehend persons who have committed a crime, conducted an act of disorder or damage to property or breached the rules and regulations of either House. In these cases, the System Operator will ensure that release meets the legal requirements.

Judgements about disclosure are made by the System Operator who has the discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or statutory information access right.

[7] This is a requirement of the Data Protection Act 1998. Further guidance on this is contained in the ICO CCTV code of practice

[8] This period is kept under review.

Once the images and information have been disclosed the receiving body, such as the police, becomes responsible for their copy of that image. Following release, it is then the recipient's responsibility to comply with any legal obligations and the Home Office Code of Practice in relation to any further disclosures.

Individuals can request images and information about themselves through a subject access request[9] under sections 7 and 8 of the Data Protection Act 1998 (Rights of Data Subjects and Others). Each application will be assessed on its own merits and general blanket exemptions will not be applied. However, in considering a request made under the provisions of section 7 of the Data Protection Act 1998, exemptions may be made by reference to section 29 of the Act which states:

> *Personal data processed for any of the following purposes:-*
>
> *i) The prevention or detection of crime*
>
> *ii) The apprehension or prosecution of offenders*
>
> *are exempt from* [the subject access provisions] *in any case 'to the extent to which the application of those provisions to the data would be likely to prejudice any of* [those matters].

Within the statutory framework provided under the Criminal Procedures and Investigation Act 1996, disclosure can also be made to defendants of material which the prosecution would not intend to use in the presentation of its own case (known as unused material). Disclosure of unused material under the provisions of this Act should not be confused with the obligations placed on the data controller by section 7 of the Data Protection Act 1998 (known as subject access).

Requests for information from public bodies may be made under the Freedom of Information Act 2000.[10]

h) Measures to safeguard against unauthorised access and use of images and information

The release of images and information for use as evidence in legal or disciplinary proceedings is subject to careful security safeguards in order to comply with legal obligations and to help foster public confidence. Images are only released after a formal request, with an auditable justification, has been made and authority has been given by either Black Rod, the Serjeant at Arms, the Yeoman Usher, the Deputy Serjeant at Arms or the Assistant Serjeant at Arms. Exceptionally, where release is time critical to control an ongoing situation, prevent crime or apprehend suspects, the Control Room Supervisor or Duty Inspector may make the authorisation but

[9] 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.
[10] Ibid.

must justify and seek confirmation of their decision from the Yeoman Usher or Deputy Serjeant Arms at the first opportunity. Images and information will only be used for the purposes set out in paragraph 9(a). The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

i) Use of the security camera systems to support public safety and law enforcement through the processing images and information of evidential value

Part of the effectiveness of the parliamentary security camera systems is their capability to capture, process, analyse and store images and information at a quality which is suitable for crime prevention, detection, investigation and prosecution. The procedural and technical safeguards help ensure the forensic integrity and reliability of recorded images and information, including any metadata (e.g. time, date and location). They also ensure that the rights of individuals recorded by the security camera systems are protected and that the material can be used as evidence in court. In order to ensure that this capability is maintained, any upgrades to existing systems or new security camera systems ensure that:

i. The images and information from the security camera systems are exportable when requested by a law enforcement agency;

ii. The export of images and information is possible without interrupting the operation of the system;

iii. The exported images and information are in a format which is interoperable and can be readily accessed and replayed by a law enforcement agency;

iv. The exported images and information preserve the quality of the original recording and any associated meta data (e.g. time, date and location).

j) Maintenance of records, information and databases

Use of technologies such as Automatic Number Plate Recognition or facial recognition systems which may rely on the accuracy of information generated elsewhere such as databases provided by others are only introduced once an assessment has been made to ensure the underlying data are fit for purpose. This not only helps ensure the reliability, accuracy and integrity of data but it protects the information by limiting its use to the purposes for which it was intended.