

---

---

## FACT SHEET

### Policy on Installation of Closed Circuit Television Systems in Public Places: the United Kingdom

#### 1. Introduction

1.1 The purpose of this fact sheet is to provide the Legislative Council Panel on Security with basic facts regarding the policy on installation of closed circuit television (CCTV) systems in public places in the United Kingdom (UK)<sup>1</sup>.

#### 2. Number of CCTV Cameras Currently Installed

2.1 The first town centre CCTV system was introduced in King's Lynn in 1987, and by 1997 CCTV systems were operational in over 300 town and city centres in England and Wales. There are more than 300 000 CCTV cameras installed in the UK for the purposes of preventing and detecting crime, protecting public and private properties, managing city centres and monitoring traffic.

#### 3. Operation of the CCTV System

3.1 The local authority (e.g. city council, borough council or parish council) and/or police is the owner/data controller of the public CCTV system installed in its area. For instance, there are more than 30 boroughs in the Great London Area.

3.2 A department/unit will be established under the data controller, which is responsible for managing the CCTV system. For example, in Greenwich Borough of London, the Council has established a Community Safety Unit for managing, operating and using the CCTV system.

3.3 The responsible department/unit sets up a CCTV control room which is operated on a 24-hour basis. The control room is capable of receiving images throughout the areas under surveillance.

#### 4. Financing the CCTV System

4.1 The data controller bears the cost of the CCTV system in its area.

---

<sup>1</sup> We have sent enquires to both the New York City Government and the Tampa City Police Department to provide information on this subject. However, as of the publication date of this fact sheet, we have not received their replies. We also cannot find detailed information on Japan.

4.2 To deal with crime and disorder in public places, the UK central government launched a Crime Reduction Programme CCTV initiative in May 1999. Under this initiative, a total of £60 million of capital funding was available to data controllers for new and extended CCTV systems in public places.

## **5. Legislation Regulating the Installation and Uses of CCTV Systems in Public Places**

5.1 In the UK, legislation regulating the installation and uses of CCTV systems in public places includes the Data Protection Act 1998 and the Human Rights Act 1998.

### Data Protection Act of 1998

5.2 The Data Protection Act 1998 provides a statutory basis for a systematic control of CCTV surveillance in public places and legally binding procedures in regulating surveillance of public places. The CCTV system is covered by the Act because part of its operation is to process images (i.e. personal data) of individuals observed by CCTV cameras.

5.3 The Information Commissioner (Head of the Data Protection Office, formerly called the Data Protection Commissioner) issued a Code of Practice to provide guidance as to good practice for users of CCTV and similar surveillance equipment.

5.4 The Code of Practice sets out the standards for a CCTV system to meet to comply with the requirements of the 1998 Act. These standards are based on the Data Protection Principles which requires that:

- (a) *"personal data shall be processed fairly and lawfully;*
- (b) *personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;*
- (c) *personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;*
- (d) *personal data shall be accurate and, where necessary, kept up to date;*
- (e) *personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;*
- (f) *personal data shall be processed in accordance with the rights of data subjects under this Act;*
- (g) *appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data; and*

- 
- 
- (h) *personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."*

5.5 To conform with the Data Protection Act:

- (a) the Information Commissioner must be notified of the ownership of the CCTV system and the purpose of setting up CCTV cameras in a particular area;
- (b) the data controller is required to place visible and legible signs so that members of the public are aware that they are entering a zone which is covered by surveillance equipment;
- (c) CCTV cameras should be sited to ensure that they avoid capturing data/images that are irrelevant or intrusive;
- (d) cameras need to be properly maintained and serviced to ensure that clear images are recorded;
- (e) tapes should be used a maximum of 12 times and retained a maximum of 31 days before re-use;
- (f) images must not be retained for longer than is necessary;
- (g) if the images are retained for evidential purposes, they should be retained in a secure place;
- (h) access to recorded images should be restricted to a manager or designated member of staff who will decide on third-party access;
- (i) all requests for access or for disclosure should be recorded;
- (j) all visitors must be authorised and recorded in the visitors' log;
- (k) if access to or disclosure of the images is allowed, then the access or disclosure date and time, identification of the third party, reason for allowing access or disclosure, and extent of the information accessed or disclosed should be documented; and
- (l) operators/staff must be trained in equipment use and tape management as well as fully aware of the codes of practice and procedures for the system.

5.6 Under the Data Protection Act 1998, the data controller of a public CCTV system is required to publish a separate code of practice to regulate the management, operation and use of the system. Copies of the code are made available to the public. Each data controller publishes its own code of practice. It is noteworthy that the details of the codes published by data controllers are more or less the same while any differences are primarily due to the ownership of the system.

---

---

*Police Access to Tapes*

5.7 If the local authority is the sole data controller, most of the times the police can still have access to tapes with authorisation and/or pre-arrangements.

*Complaints*

5.8 Under a formal complaint procedure established by the data controller, the public can address complaints about the operation of the system to the data controller. Copies of the complaint procedure are made available to the public.

*Breaches of the Code of Practice*

5.9 Any breach of the code by control room staff will be investigated by a senior staff with the data controller in order for him to take the appropriate disciplinary action. A serious breach may warrant an independent investigation, and recommendations may be made on how the breach can be remedied.

*Review and Evaluation*

5.10 The code is subject to a full review on a regular basis (e.g. every two years). Any major changes to the code may only take place after public consultation.

Human Rights Act of 1998

5.11 To protect the privacy of the public, the data controller is also required to comply with Article 8 of the Human Rights Act 1998, which states that "*everyone has the right to respect for private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as 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 or freedom of others.*"

5.12 To comply with Article 8 of the Human Rights Act of 1998, the data controller has to achieve a balance between the needs of society and the rights of the public.

---

Prepared by Mr Jackie WU  
28 March 2002  
Tel: 2869 7735

---

*The Legislative Council Secretariat welcomes the re-publication, in part or in whole, of this document, and also its translation in other languages. Materials may be reproduced freely for non-commercial purposes, provided acknowledgement is made to the Research and Library Services Division of the Legislative Council Secretariat as the source and one copy of the reproduction is sent to the Legislative Council Library.*

---

---