evidence of delivery. (Some data controllers may require the notarisation of the letter to legally establish identity.)

Data Protection Act 1998; 1998 Chapter 29, Part II Section 7(2)
A data controller is not obliged to supply any information under subsection (1) unless he has received –
(a) a request in writing, and
(b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

The filmmaker is to allow a maximum 40 days after sending the data request for an initial response.

Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
A data controller must comply with a subject access request promptly, and in any event within forty days of receipt of the request or, if later, within forty days of receipt of: the information required (i.e. to satisfy himself as to the identity of the person making the request and to locate the information which that person seeks); and the fee.

The filmmaker is to establish a set of rules for handling the various formats in which the data may be sent (video tape, DVD-video, digital files encoded with proprietary codecs, hard copies of frames, etc.).

5. SOUND

CCTV systems are not permitted to record sound. The filmmaker is to establish a set of rules for the soundtrack (if any) of the movie.

6. DISTRIBUTION

Footage received is subject to complex copyright issues. The filmmaker is to take legal advice and establish a strategy.

* * *

the filmmaker as symbiont:
opportunistic infections of the surveillance apparatus

Manifesto for CCTV filmmakers declares a set of rules, establishes effective procedures, and identifies issues for filmmakers using pre-existing CCTV (surveillance) systems as a medium in the UK. The manifesto is constructed with reference to the Data Protection Act 1988 and related privacy legislation that gives the subjects of data records access to copies of the data. The filmmaker's standard equipment is thus redundant; indeed, its use is prohibited. The manifesto can be adapted for different jurisdictions.

* * *

MANIFESTO FOR CCTV FILMMAKERS

1. GENERAL

The filmmaker is not permitted to introduce any cameras or lighting into the location.

2. SCRIPT

A protagonist ("data subject") is required to feature in all sequences.

Data Protection Act 1998; 1998 Chapter 29; Part II Section 7(1).
[A]n individual is entitled –
(a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,
(b) if that is the case, to be given by the data controller a description of –
    (i) the personal data of which that individual is the data subject,
    (ii) the purposes for which they are being or are to be processed, and
    (iii) the recipients or classes of recipients to whom they are or may be disclosed,
(c) to have communicated to him in an intelligible form –
    (i) the information constituting any personal data of which that individual is the data subject, and
    (ii) any information available to the data controller as to the source of those data,
(d) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

The documented activity of the protagonist must qualify as personal or sensitive data. The filmmaker is to establish this by locating a CCTV camera and circumscribing the field of action for the actors relative to it, so that incidents of biographical relevance (i.e., that reveal personal data) occur in the frame.

ICO CCTV systems and the Data Protection Act JB v.5 01/02/04
2. The court decided that for information to relate to an individual (and be covered by the DPA) it had to affect their privacy. To help judge this, the Court decided that two matters were important: that a person had to be the focus of information, the information tells you something significant about them.

The provisions of the 1998 Act are based on the requirements of a European Directive, which at, Article 2, defines, personal data as follows:
"Personal data" shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
The definition of personal data is not therefore limited to circumstances where a data controller can attribute a name to a particular image. If images of distinguishable individuals' features are processed and an individual can be identified from these images, they will amount to personal data.

All people other than the protagonist ("third parties") will be rendered unidentifiable on the data obtained from the CCTV operators. Typically, operators blur or mask out faces of third parties. The filmmaker is to consider the visual impact of this manipulation, and to establish a rule for the handling of footage delivered with ineffectual masking or blurring – for example, reporting the offence.

Right to Privacy in Article 8 of the Human Rights Act 1998:
RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE
1. Everyone has the right to respect for 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 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 freedoms of others.

DPA1998
4. On the other hand, the disclosure of third party information in compliance with a subject access request may also expose the data controller to complaint or action by the third party, for example [...] for breach of confidence.
6. The data controller should consider to what extent it is possible to communicate the information sought without disclosing any third party information [...] This might be achieved by editing the information to remove names or other identifying details.

3. LOCATION

The filmmaker is to choose locations covered by multiple cameras operated by a large business, private security firm or public authority – or, if operated by a small retailer, cameras that can be panned or zoomed remotely. Locations may be mobile (e.g., public bus).

ICO CCTV systems and the Data Protection Act JB v.5 01/02/04
If you have just a basic CCTV system your use may no longer be covered by the DPA.
[...] Small retailers would not be covered who
– only have a couple of cameras,
– can't move them remotely,
– just record on video tape whatever the camera picks up,
– only give the recorded images to the police to investigate an incident in their shop.

For every camera, the operator's name and contact details are to be noted.

Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
7. Signs should be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment.
The signs should contain the following information:
Identity of the person or organisation responsible for the scheme.
The purposes of the scheme.
Details of whom to contact regarding the scheme.
(First Data Protection Principle).

4. FOOTAGE REQUESTS

After each shoot, the filmmaker is to send a written request ("subject access request letter") to the CCTV operator ("data controller") to ensure that the data recovery process can be initiated while the recordings are still archived. (Mandatory retention periods vary.)

Code of practice issued by the Data Protection Commissioner, under Section 51(3)(b) of the Data Protection Act 1998, 07/2000
1. Once the retention period has expired, the images should be removed or erased (Fifth Data Protection Principle).

The subject access request letter is to state the place and time of the recording and include a picture of the protagonist (wearing the same clothes if possible) and a cheque for £10 (the maximum fee chargeable). Letters should be sent by a secure system that provides