

Submission by Liberty to the Data Protection Registrar's consultation on the draft Code of Practice for CCTV

Contents

- 1 Introduction**
- 2 General principles**
- 3 Data control**
- 4 Timing**
- 5 Maintenance**
- 6 Processing and security**
- 7 Access by data subjects**
- 8 Conclusion**

1. Introduction

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaign and research. It is the largest organisation of its kind in Europe and is democratically run.

It has a long standing interest in the protection of personal privacy in general and data protection in particular. Liberty has published several reports on the subject. These have concerned both the Council of Europe Convention and the Data Protection Act 1984 and more recently the Data Protection Act 1998. Liberty's legal department has experience in advising individuals about Data Protection Law and in making applications to the Data Protection Registrar.

Liberty has been calling for proper statutory regulation of CCTV systems for at least twenty years. Whilst we welcome this Code of Practice it is no substitute for such regulations and we are concerned that it will have little effect on the kind of abuse detailed so clearly in "The Maximum Surveillance Society: The Rise of CCTV", Clive Norris and Gary Armstrong, 1999. In addition, the absence of proper regulation the interference with privacy created by CCTV may well violate the right to privacy which will part of domestic law once the Human Rights Act comes into force in October 2000.

This document is in response to a draft document for consultation in relation to the use of CCTV and similar surveillance equipment. The proposed Code of Practice is issued by the Office of the Data Protection Registrar in accordance with powers under Section 51(3)(b) of the Data Protection Act 1998 (the 1998 Act). References to page numbers are to the corresponding page in the proposed Code of Practice.

Liberty welcomes the introduction of a Code of Practice in relation to the use of CCTV surveillance equipment. Its use in public places gives rise to a complex balance between the rights of data subjects who are engaged in private activities (e.g. shopping) albeit in public spaces and the rights of data controllers whose surveillance is directed at one or more aspects of the public interest which may well include the preservation of certain rights (e.g. safety) of the data subjects themselves.

The conflict between the competing rights in this area is likely to be fairly stark. It is therefore Liberty's view that the Code of Practice would be more effectively introduced were compliance with it a requirement of the 1998 Act. That this is not the case is something of a missed opportunity.

Liberty notes that the Code is not intended to be used by official law enforcement bodies, such as the police force, security service or Customs & Excise when carrying out specialised and/or covert surveillance or operations. Liberty does not accept that these areas should

remain outside the scope of any relevant Code of Practice. Indeed there may well be a pressing need for such agencies to develop codes of practice governing specialised investigations and/or surveillance in particular.

Liberty confines its observations to the proposed Code of Practice which is substantially found in the first part of the draft document for consultation. The second part of the document merely sets out in fairly discursive form interpretations of various provisions of the 1998 Act. It is very difficult to know whether the full implications of the Act in relation to CCTV surveillance operations have been spelt out in the draft document but what follows is a response to the substance of the proposals themselves.

In relation to the timetable for review of the Code of Practice, regular review is obviously essential. It would considerably strengthen confidence in the Code of Practice if a set timetable for review and/or revision were set down in the Code of Practice itself. As the potential range of operations and data controllers is so wide it is inevitable that practical problems will need to be addressed and it seems sensible for the Code to be sufficiently flexible to be capable of amendment in a systematic manner according to a set timetable.

2. General principles

The new Code of Practice needs to incorporate a set of general principles (other than the Data Protection principles) to govern its operation.

The first principle is that all operators of CCTV systems whose systems need to comply with the provisions of the Act should carry out some sort of "Data Protection Audit". Such an exercise would be not unlike a risk assessment under health and safety legislation where those responsible for a company's or institution's policy in a particular area undertake an analysis whereby compliance with the legal obligations can be assessed and monitored.

Such an assessment should include a particular emphasis on those areas where the system is most likely to be found to be in contravention of the provisions of the Act or at least highlighting those aspects of the surveillance system which give rise to the greatest dangers of non-compliance.

All such operators should include in such a risk assessment the assessment recommended on page 4 as to the appropriateness of and reasons for using CCTV or similar surveillance equipment. This will make notification of the said purpose to the Data Protection Commissioner a relatively easy task. It would also cause data controllers to bring into existence a readily identifiable set of documents against which the person or organisation responsible for the system can be judged.

Such a risk assessment would include consideration of the siting of cameras as recommended on page 5. Liberty broadly welcomes the standards proposed in relation to the siting of cameras. It is particularly important that signs should be placed in the vicinity of the cameras so that the public are aware that they are entering zone which is covered by surveillance equipment. Signs should be sufficient in number and sufficiently large and visible to enable this to happen.

Sinage

A minimum size of A3 might well in certain circumstances be too small and data controllers ought to be encouraged to provide signs as large as say A2 where this is practicable. If signs are too small and contain too much information they are likely to be substantially ignored and/or to be passed over even by interested members of the public.

It is difficult to see why the requirement on page 6 (that information obtained from areas where no signs have been posted should not be retained and used for any other purpose) should not be a mandatory requirement. Similarly such equipment must not be used to

record conversations between members of the public in order fully to respect the first and third Data Protection principles.

3. Data control

Liberty welcomes the emphasis on page 7 of "purpose sensitivity" that is to say a requirement that data controllers assess the surveillance system by reference to the purpose to be achieved. The principle whereby unnecessary information should not be gathered should be clearly and distinctly stated in this section. This is the more important given the understandable need to ensure that such information as is gathered is itself of sufficiently high quality to be useful.

4. Timing

The question of timing is important and should be separately addressed. The principle which the Code of Practice should seek to uphold is that recording should take place for no longer than is necessary. The necessity for recording is to be determined by reference to the particular purpose.

5. Maintenance

As a requirement of fulfilling the Third, Fourth and Fifth data protection principles insofar as they are concerned with the quality of personal data, the Code of Practice should recommend the keeping of a maintenance log as a matter of best practice. The purpose behind this is twofold. It ensures adequate maintenance of equipment in working order and provides evidence (for possible future use) of regular monitoring/maintenance of the equipment where for example its accuracy is sought to be impugned in legal proceedings.

6. Processing and security

In relation to processing of images Liberty welcomes the principle underpinning this section on page 9 whereby images which are not required for the purposes of the scheme should not be retained for any longer than is necessary.

The security requirements of images is addressed on page 9. The security of images including the requirement to restrict access to images to designated staff is but one aspect of a general principle whereby operators should be encouraged by the Code of Practice to educate and train the relevant members of their work force in relation to all aspects of Data Protection including primarily compliance with the Code which should set out (either as an Appendix or otherwise) the eight data protection principles, as well as the standards sought to be upheld, in readily intelligible language. The purpose behind requiring data controllers not only to restrict access to information but to ensure those who do have access to data obtained from surveillance equipment are sufficiently well versed in the practicalities of compliance, is that the ability of data controllers effectively to protect the rights of data subjects will depend upon the knowledge and training of employees on a practical day to day level. In particular the Code should ensure that viewing of recorded images should not be possible from non-restricted areas and that recorded images should only be visible in a restricted area.

It follows that Liberty's view is that the recommendation that all operators and employees with access to images should be aware of the procedures which need to be followed. In this regard the Code needs to be strengthened by reference to a general educational and training principle with its own set of standards in relation to:

- (a) the general data protection principles to be respected and complied with in the operation of a system;
- (b) the importance of a data subject's rights;
- (c) the need to make sure that the system goes no further than is necessary to achieve the

purpose;

(d) restrictions on access to information (including the procedures in relation to third party access;

(e) the need to ensure that equipment is properly maintained;

(f) the proper procedures for safe removal or disposal of images and/or data;

In relation to the proposals under "Access to and Disclosure of Images to Third Parties". It is of very considerable importance that where images are disclosed to the media, the images of individuals need to be disguised or blurred and that this provision on page 12 should be strengthened to include a requirement that the blurred or disguised images are such that the individuals are not readily identifiable. If the data controller system does not have the facilities to carry out this type of operation then disclosure must not take place unless this is effectively subcontracted to another party with the appropriate guarantees listed in subparagraphs (a) to (e) on page 12.

7. Access by data subjects

The procedure whereby data subjects are entitled to request access to information gathered would be greatly strengthened by a positive obligation of education and training of employees. This would considerably improve the ability of data controllers in effectively to deal with requests from data subjects.

In terms of response times the provision on page 15 should be strengthened to require the manager or designated member of staff to provide a written response to the individual as soon as is practical and in any event within 21 days of receiving the request.

Where an individual requires an automated decision to be reconsidered the Code of Practice should provide that the reconsideration will take place as soon as is practicable and in any event within 21 days of the request being received. The reconsidered decision should also document the matters listed in sub paragraph (a) to (c) on page 16 and the reasons relied upon in support of the reconsidered decision, whether the original decision is upheld (in whole or in part) or not.

In relation to the contact point for members of the public, it is of very considerable importance that this contact point is effective. It is of comparatively little use if the number is a general number where the switchboard or reception is unaware of the nature of the enquiry being made or the proper destination for the enquiry in the organisation. Again effective training and education provisions should include an obligation to provide effective recourse to a suitably trained and knowledgeable employee where practicable.

Liberty welcomes the proposal for an annual report to be produced evaluating the effectiveness of the surveillance system.

8. Conclusion

Liberty welcomes many of the proposals contained in the draft document and in particular welcomes the emphasis in the Code on respect for the data protection principles and the proposals whereby the use and operation of CCTV surveillance systems is continually made subject to a test of practical necessity. This is a principle which ought to be clearly stated as one of the general principles underpinning the Code of Conduct against which the system as a whole ought to be tested inter alia in the annual report recommended on page 17.

This document sets out Liberty's observations in relation to part 1 of the draft document. The major criticism is a failure to set out general principles which can then be used to underpin particular standards. The regime could be considerably strengthened by introducing a requirement that data controllers undertake a risk assessment and a requirement that education and training assume a higher priority.

Liberty, April 2000