CCTV

- Domestic CCTV 01.03.07

Domestic CCTV

Background

As CCTV and surveillance equipment becomes more readily available the Commissioner receives more and more calls relating to it's use by 'private' individuals. The most common complaint is the apparent monitoring of one resident in a street by another, usually in a neighbouring property.

Line to take

Key Points

- In these situations the Act is unlikely to apply due to section 36, the 'domestic purposes exemption'.

- Section 36 states that:

'personal data processed by an individual only for the purposes of that individuals personal, family or household affairs (including recreational purposes are exempt from the data protection principles and the provisions of parts II and III'.

- As the monitoring of a residential property is clearly going to fall under the category of 'personal, family' or household purposes' the Act will not apply. This would be the case even if the cameras were to stray beyond the boundaries of the residential property. The critical point is that the 'purpose' for which the cameras are in place is 'peronal, family or household'.

However, many complainants argue that the monitoring conducted by their neighbour cannot be for domestic purposes because they are the focus of it.

- It is important to remember that the focus of the camera is not the issue, it is the purposes of the monitoring and the fact that those doing the monitoring are not classed as a data controller (as defined in the Act) that 'triggers' the section 36 exemption.

- Individuals should be advised that although the DPA is unlikely to apply, other legislation in the area of 'anti-harrassment' or 'anti-social behaviour' MAY do. and consequently they should seek their own independent legal advice.
-

- CCTV - LTT re status of C.O.P. vs p/d paper

CCTV (non-domestic)

Background

Prior to our revised line on 'what makes data personal' and the new CCTV code of practice (released on the 28 January), advising about personal data and CCTV could be difficult. However the revised CCTV COP is compatible with our revised view of personal data and the situation is now more straight forward. The new CCTV COP is primarily aimed at businesses and organisations who routinely capture images of individuals on their CCTV equipment. Broadly our view is that those CCTV images where an individual can be identified are likely to be considered as personal data. As such all the usual provisions of the DPA 1998 will apply, including subject access rights and the obligation to notify.

Line to take

It is essential that you familiarise yourself with our lines to take in our new CCTV Code of Practice. Please follow the link:

CCTV Code of Practice Revised Edition 2008 (released 28th January 2008)

Any callers asking about the data protection Act and CCTV can be referred to our COP. However it should be noted that whether a camera can 'zoom, pan or tilt', is no longer relevant. It is whether the cameras are capturing personal data that is the important factor when deciding if the Act would apply.

It is also important to note that our view regarding 'small business users' and their obligation to notify has been revised.

CCTV small business users and notification

Although there is not a specific definition of a 'small business user' in the COP, we would take this to mean a data controller who is a small to medium sized organisation and uses a very small number of CCTV cameras.

We have reached agreement with the MoJ about the line to take on notification of small CCTV users. This applies to small CCTV users who now come within the scope of the DPA because of our revised interpretation of the definition of personal data but who in the past we would have told that they do not need to notify. It is:

- we have raised with the MoJ the possibility of introducing a notification exemption for small business users of CCTV.
- the MoJ have agreed that, in principle, the proposal to introduce a

notification exemption is sensible and we are now working with the MoJ on how best to address this.

- in the meantime, pending the introduction of a statutory exemption, the ICO has no plans to actively pursue small business users of CCTV who have not yet notified.
- Although the ICO has no plans to actively pursue small business users of CCTV who have not notified it is important to note that the images captured are still classed as personal data and therefore their other obligations under the DPA 1998 would still apply in terms of how they process the data..

- CCTV in classrooms 12.02.09

CCTV in Classrooms

Background

The Information Commissioner has received enquiries from individuals regarding CCTV in classrooms, and in particular, about an organisation called Classwatch. In essence Classwatch are marketing a technology; it is for schools to decide whether their use of such a system is proportionate and reasonable.

Line to take

The ICO advises that:

- Schools seeking guidance on this issue should consult our CCTV Code of Practice. This makes it clear that organisations will have to consider very carefully whether use of any surveillance system is necessary to address a pressing need, such as public saftey and crime prevention; whether it is proportionate to the problem it is designed to deal with, whether it is justified in the circumstances and whether people know it is going on.

- We recognise that CCTV surveillance is a sensitive issue, particular when children are involved. For that reason, schools should consult parents when making any decision to use such a system.

NB If dealing with a written enquiry please copy the line to take above

- Forced CCTV in pubs 29/06/08

Forced CCTV in pubs

Background

The ICO has become aware of some police forces forcing landlords to install CCTV in pubs as a licensing requirement.

Line to take

- Imposing a blanket condition that all pubs should install CCTV as a mandatory licensing requirement raises serious privacy concerns.

- We recognise that CCTV plays an important role in the prevention and detection of crime and can help to reduce crime in areas of high population density, such as city boroughs. However, we are concerned at the prospect of landlords being forced into installing CCTV in pubs as a matter of routine to meet the terms of a licence.

- Installing surveillance in pubs to combat specific problems of rowdiness and bad behaviour may be lawful, but hardwiring in blanket measures where there is no history of criminal activity is likely to breach data-protection requirements.

- Local police forces and licensing authorities should not demand CCTV as a "default" condition but should consider each licence application on a case by case basis.

- Use of CCTV must be reasonable and proportionate if we are to maintain public trust and confidence in its deployment.

- CCTV signage where there is a potential detriment to individuals by identifying the data controller 11.11.10

CCTV signage where there is a potential detriment to individuals by identifying the Data Controller

Background

To be used in situations where identifying the organisation operating CCTV may cause potential detriment, for example outside a women's refuge or mental health care accommodation.

Line to take

We recognise the balance to be struck between the privacy rights of the individuals residing in these properties and those of the wider community.

The CCTV Code of Practice outlines the general requirements under the Data Protection Act 1998 (the DPA) as follows:

"9.1 Letting people know

You must let people know that they are in an area where CCTV surveillance is being carried out. The most effective way of doing this is by using prominently placed signs at the entrance to the CCTV zone and reinforcing this with further signs inside the area. This message can also be backed up with an audio announcement, where public announcements are already used, such as in a station.

Clear and prominent signs are particularly important where the cameras themselves are very discreet, or in locations where people might not expect to be under surveillance. As a general rule, signs should be more prominent and frequent where it would otherwise be less obvious to people that they are on CCTV.

In the exceptional circumstance that audio recording is being used, this should be stated explicitly and prominently.

Signs should:

• be clearly visible and readable;
• contain details of the organisation operating the system, the purpose for using CCTV and who to contact about the scheme (where these things are not obvious to those being monitored); and
• be an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

Signs do not need to say who is operating the system if this is obvious. If

CCTV is installed within a shop, for example, it will be obvious that the shop is responsible. All staff should know what to do or who to contact if a member of the public makes an enquiry about the CCTV system. Systems in public spaces and shopping centres should have signs giving the name and contact details of the company, organisation or authority responsible.

- Do you have signs in place informing people that CCTV is in operation?

- Do your signs convey the appropriate information?"

In the majority of circumstances we would expect organisations to abide by the Code of Practice but there is a degree of discretion and we recognise that there will be exceptions.

The aim of CCTV signage is to provide people with information about who is capturing their image and for what purposes (providing fair processing information) which is requirement of the first principle of the DPA.

Although in the majority of cases signage will be the most appropriate method of letting people know that CCTV is in operation, this is not the only way to communicate this information to individuals. In limited circumstances, such as those you have outlined, it may be that there are good reasons that another way of providing people with fair processing information, or at least some elements of fair processing information, is more appropriate.

The First Principle of the DPA requires that the following fair processing information is provided:

(a) the identity of the data controller,
(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
(c) the purpose or purposes for which the data are intended to be processed, and
(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

Where it is not obvious who is operating the system and it is possible that providing the identity of the data controller (_____) on CCTV signage may have a detrimental effect on individuals who are residing at the premises, the DPA will not dictate that this information must be provided on a CCTV sign. However, the information must be made readily available in some other form and alternative measures should be put in place.

In these circumstances a CCTV sign should provide individuals with the following information:

- That CCTV is in operation.
- The purpose of the CCTV if this is not obvious (ie on a building people will

generally expect the purpose for the camera is crime prevention).

• A contact telephone number or address where an individual can write to exercise their rights under the DPA.

If the information outlined above is provided then any individual captured by the CCTV cameras would be able to contact you to obtain the other fair processing information they may require to exercise their rights under the DPA. The additional fair processing information will have been made readily available if the organisation can provide the following over the telephone or when replying to a letter:

• The identity of the data controller.

• Any further information which is necessary to make the processing fair.

This approach is limited to circumstances where there are clear reasons why providing the name of the data controller on CCTV signage would be detrimental to individuals.

- Community CCTV schemes (access to footage) 31/10/11

Community CCTV schemes (access to footage)

Background

We sometimes receive requests for advice from housing authorities regarding the operation of CCTV systems where the footage is accessible to residents (usually through being streamed to monitors within individual flats).

Line to take

Depending on the existing level of understanding of the DPA, you may need to explain the general principles and highlight the requirements of the CCTV Code of Practice (http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx).

- Advise that the ICO cannot give formal approval to such a scheme. It is for the housing association, as the data controller, to decide whether it is possible to introduce such a scheme in compliance with the Data Protection Act.

- The housing association, as the data controller, would need to be clear about the purpose of the proposed scheme. They would need to determine whether such a system is justified, taking into account what benefits could be gained and consider overall whether this would be the most appropriate way to be dealing with the security of the housing and the prevention of crime.

- They should consider the level of impact it is likely to have on people's privacy; and how such a scheme would operate in practice – in particular, how they would comply with the DPA's principles.

- If residents had access to the footage then our main concerns would be the fact that residents could potentially view distressing footage if there was no authorised person viewing the footage to enable the system to be shut down when required. We would also be concerned if the residents have the facility to record any images they view.

31/10/11