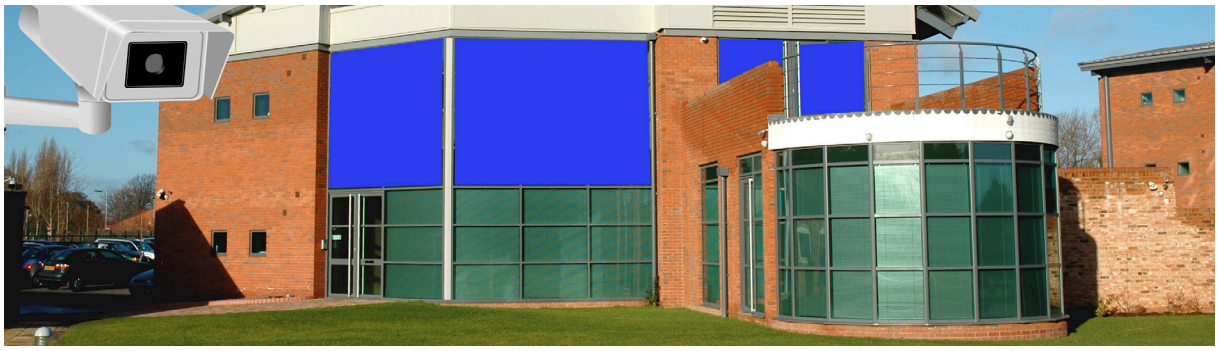
bsia
british security industry association

CCTV
privacy masking
– a guide



August 2016

For other information please contact:

British Security Industry Association
t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

Form No. 197 | Issue 2

Contents

1. The need for privacy masking

'Privacy Masking' is the common term covering the need to restrict what can be seen by means of Closed Circuit Television (CCTV) systems. It applies equally to images displayed live for surveillance purposes and images recorded for later use. Along with the guidance of the Surveillance Camera Commissioner's - Surveillance Camera Code of Practice there are a number of pieces of UK legislation that determine the legal requirements for privacy masking, including the Human Rights Act 1998 and the Data Protection Act 1998.

1.1. The Human Rights Act 1998 (HRA)

The HRA implemented in the UK gives fundamental rights and freedom to everybody, this Act is based on the European Convention on Human Rights (ECHR) and in Article 8 it states that:

"Everyone has the right to respect for his private and family life, his home and his correspondence".

1.2. The Data Protection Act 1998 (DPA)

The DPA places obligations on people and organisations who hold and use personal data. The DPA sets out eight data protection principles that state the data must be:

1. Used fairly and lawfully;
2. Used for limited, specifically stated purposes;
3. Used in a way that is adequate, relevant and not excessive;
4. Accurate;
5. Kept for no longer than is absolutely necessary;
6. Handled according to people's data protection rights;
7. Kept safe and secure;
8. Not transferred outside the European Economic Area without adequate protection.

Cameras attached to a private individual's home viewing beyond the property boundary may, in certain circumstances (without privacy masking), no longer be exempt from the requirements of the DPA under section 36.

To assist in the application of these Data Protection Principles within the operation of CCTV systems, the Information Commissioners Office (ICO) published 'In the picture: A data protection code of practice for surveillance cameras and personal information' in 2015. This code also reflects the wider regulatory environment. When using, or intending to use, CCTV systems many organisations also need to consider their obligations in relation to the Freedom of Information Act 2000 and the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act.

1.2.1. Surveillance Camera Commissioner's - Surveillance Camera Code of Practice (SCCoP)

The role of the Surveillance Camera Commissioner (SCC) is to encourage compliance with the surveillance camera code of practice. The office of the commissioner was created under the Protection of Freedoms Act 2012 to further regulate CCTV.

Under the act the SCC has produced the SCCoP that sets out twelve guiding principles that should be adopted by system operators, the key points that relate to masking (or privacy) are:

- **Principle 2:** The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

- **Principle 6:** No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

- **Principle 10:** There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

In addition there may be other legislation that will affect aspects of camera installation such as the Town and Country Planning Order 1995. These may not impact on DPA or HRA issues directly, but may limit how a CCTV system may be installed. Consideration should also be given to other byelaws introduced by local government. These will vary from region to region.

2. Methods of restricting camera views

A CCTV system should be designed to limit its coverage so that it does not cover areas or 'spaces' which are outside its intended use. When designing a system, the spaces to be surveyed and those surrounding it should be considered from a DPA, HRA and the SCCoP perspective and the level of privacy for each space determined. Should camera fields of view need to overlap one or more of the surrounding spaces, then action must be taken to comply with the DPA, HRA and the SCCoP requirements.

Note: With analogue or lower resolution IP cameras 4-CIF, 1 or 2MP cameras, where viewing an image with a target object at a distance is too small (or when digitally zoomed in, is unrecognisable), a specific privacy zone may not be necessary i.e. as the resolution increases object recognition at distances becomes more of an issue.

There are various methods by which DPA, HRA and the SCCoP restrictions may be satisfied. One approach is through the select positioning of the cameras to be used to ensure that private or public space cannot be seen. Where the camera field of view does infringe on a private or public space, either written permission from the person who owns or resides in that space should be obtained, or physical or electronic image masking should be employed.

2.1. Camera positioning

The most effective way to restrict the field of view of a camera is by careful selection of camera position and lens field of view to prevent the camera from overlooking private areas. With fixed cameras this can be relatively straightforward, but with functional cameras this may involve setting movement limits either physically or within the control system's settings to restrict the horizontal and or vertical rotation of the camera and associated equipment. If control system settings are used to limit the field of view, it is important to make sure that these are protected via a key switch or pass code so that they cannot be subsequently altered or overridden by unauthorised persons.

2.2. Masking

The type of masking used should ensure that, when in force, the area to be restricted from view remains private. There are currently two main types of masking, these are:

2.2.1. Physical masking

External physical barriers such as walls, embankments or trees and vegetation in combination with camera positioning can be used to mask the views of private or public areas. However, it is important to remember and take into account that the coverage provided by vegetation may vary due to seasonal changes, growth and pruning.

2.2.2. Electronic masking

There are several ways that electronic masking may be applied. The most typical takes place in or close to the camera but could also be within the recording device subsequently allowing authorised users access to the masked part of the image. In either case the mask must always be correctly applied when required. Masks can be applied in various ways depending on the DPA, HRA and the SCCoP limitations. Masked areas of the image are commonly referred to as 'Zones'. Examples include:

a. Masked areas (usually rectangles) of solid, uniform colour so that no detail or movement in the scene covered by them can be seen through them.

b. Masks that blur or pixelate the image so that they cover to allow movement, but no fine detail to be seen, such that targets can still be tracked or incidents detected in areas covered by the masks.

c. Masks that engage only when the camera zooms in on an area, using the diminutive size of an object when far away to conceal detail.

With controllable cameras there is a need to dynamically adjust the size and position of the zone in accordance with motion control unit and zoom functions. Maintaining the integrity of the privacy masking system is important, such that its configuration can be protected to prevent settings being altered, bypassed or overridden by unauthorised persons.

There are several factors affecting the accuracy of electronic masking. On functional cameras, mask size and shape needs to automatically adjust in order to cope with changes in perspective as the camera moves.

This issue becomes more acute with the degree that the camera is tilted, especially in cases where the areas to be masked fall well below the horizon of the camera. The suitability of the electronic privacy masking method should be verified prior to the procurement and installation of equipment. Other factors that can affect the privacy masking are:

a. The speed of mask drawing and updating due to the capabilities of the hardware being used to generate the masks. This can result in the mask lagging a short time behind changes in the image due to the camera moving.

b. The resolution and accuracy of feedback of motion control unit and zoom position to the mask generator. This can result in the mask shifting towards one of the sides of the privacy zone, which in turn may result in part of the private or public area becoming visible. Making the masks slightly larger than the actual area that is required to be masked when setting them up usually compensates for this.

c. The calibration and setup of generic privacy mask generators designed for use in conjunction with a range of cameras, lenses and motion control units. Where the privacy masking system is not integral to the camera unit some form of calibration is normally required for the privacy marking to work correctly.

Where the privacy masking is applied either in the camera module, or within a dome camera assembly that is supplied complete with camera, calibration is not usually required as all necessary parameters are factory set.

Where systems require calibration, the accuracy of that calibration is normally critical to the subsequent accuracy of the privacy masking. Calibration should therefore be carried out carefully in accordance with the instructions and, if necessary, training sought from the manufacturer of the equipment. The calibration should particularly take into account the non-linearity of the zoom lens (i.e. the amount that a fixed point in the centre of the scene moves in the image as the lens is zoomed in and out).

3. References

Surveillance Camera Code of Practice Pursuant to Section 29 of the Protection of Freedoms Act 2012

The Surveillance Camera Commissioner's - Surveillance camera code of practice
www.gov.uk/government/uploads/system/uploads/attachment_data/file/282774SurveillanceCameraCodePractice.pdf

The Information Commissioners Office (ICO) - In the picture: A data protection code of practice for surveillance cameras and personal information
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

The Data Protection Act 1998
www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

The Human Rights Act 1998
www.legislation.gov.uk/ukpga/1998/42/pdfs/ukpga_19980042_en.pdf

European Convention on Human Rights (ECHR)
www.echr.coe.int/Documents/Convention_ENG.pdf

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Council of Europe, Rome 4. XI. 1950
www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765

This document was created by the CCTV Section of the British Security Industry Association (BSIA).

The British Security Industry Association is the trade association for the private security industry in the UK. Our members provide over 70% of UK security products and services and adhere to strict quality standards.

CCTV has had a profound impact on crime prevention and detection. The UK leads the way in the application of CCTV and its use is wide-ranging, encompassing facial-recognition technology, remote video monitoring, video smoke detection, mobile systems and Automatic Number Plate Recognition (ANPR) as well as many other functions.

In order to provide guidance and simplification in the complex area of CCTV, the BSIA is very active in the European & International standards arenas and also develops its own guides and codes of practice where currently standards do not exist.

The CCTV section encourages debate on new developments and concerns, such as digital video evidence and facilitating communication protocols between different manufacturers' products. In doing so it seeks to ensure that all stakeholder interests are represented including: security companies, users, the police, inspectorates and insurers.

As a security company, BSIA membership will raise your company profile and ensure that your business is at the heart of influencing the future of the security industry. You will become part of a unique group of high quality and professional companies which are well-respected and well-represented to government, end users, specifiers, standards and legislative bodies. For more information contact the BSIA.

BSIA Ltd
Kirkham House
John Comyn Drive
Worcester
WR3 7NS

t: 0845 389 3889
e: info@bsia.co.uk
www.bsia.co.uk

@thebsia

bsia
british security industry association