Video Surveillance System Privacy Masking

A guide

Contents

1. The need for privacy masking

Privacy masking is a technique used to protect individuals' privacy in video footage captured by a video surveillance system (VSS). It involves selectively obscuring or blurring certain areas of the video feed to prevent the identification of individuals or the disclosure of sensitive information.

Privacy masking is typically used when cameras are installed in public areas or workplaces where people may reasonably expect privacy. The masking process involves using specialised software to identify and blur specific areas of the video feed. This software can recognise and mask features like faces, license plates, or sensitive documents.

The software can be configured to recognise objects and blur them continuously, or it can be programmed to detect objects and blur them only when they are in motion. One of the key benefits of privacy masking is that it allows organisations to comply with privacy regulations and protect the privacy rights of individuals. In some cases, privacy masking may even be a legal requirement. For example, in the European Union, the General Data Protection Regulation (GDPR) mandates that organisations protect the privacy of individuals by using techniques like privacy masking.

Privacy masking can also protect sensitive information visible in VSS footage. For example, suppose a VSS camera is installed in a laboratory where sensitive experiments are conducted. In that case, privacy masking can obscure any information that could be used to replicate the experiments.

However, privacy masking does have some limitations. For example, it may be ineffective in situations where the video feed could be of better quality, or the camera is positioned at an awkward angle. Additionally, privacy masking may not be effective when individuals wear masks or other forms of facial covering that could obscure their identity.

In summary, VSS privacy masking is an essential technique for protecting the privacy rights of individuals and complying with privacy regulations. It involves the selective blurring or obscuring of some regions of the video feed to prevent the identification of individuals or the disclosure of sensitive information. While privacy masking has some limitations, it is an effective tool for safeguarding privacy in various settings.

2. Human Rights Act and Privacy Masking

VSS privacy masking must be balanced against Article 8 of the Human Rights Act (HRA), which protects an individual's right to respect for their private and family life, home, and correspondence.
Under Article 8 of the HRA, everyone has the right to respect their private life and home, including control of the use and dissemination of information about oneself. When VSS is used in public spaces, it can interfere with an individual's right to privacy. This is especially true when VSS is used in areas where individuals have a reasonable expectation of privacy, such as in changing rooms, restrooms, or private offices.

However, Article 8 is not an absolute right and can be balanced against other rights and interests, such as the public interest in maintaining effective surveillance for security and safety purposes. The use of privacy masking in VSS surveillance is one way to balance the right to privacy with the need for effective surveillance.

To ensure that privacy masking is balanced against Article 8 of the HRA, it is important to consider the proportionality of the surveillance measures used. This involves balancing the need for surveillance against the potential interference with individuals' privacy rights. The use of privacy masking must be proportionate to the risk being addressed, and it must be used only to the extent necessary to protect individuals' privacy rights.

Furthermore, it is important to ensure that privacy masking is not used in a discriminatory manner. This would involve using privacy masking that disproportionately affects certain groups, such as individuals, based on race, ethnicity, or religion. Such use of privacy masking would violate Article 8 of the HRA and would be inconsistent with the principles of equality and non-discrimination.

In conclusion, the use of VSS privacy masking must be balanced against the requirements of Article 8 of the HRA to ensure that individuals' privacy rights are respected. This involves considering the proportionality of the surveillance measures being used and ensuring that privacy masking is not used in a discriminatory manner. By carefully balancing these considerations, it is possible to use VSS privacy masking in a way that is effective, proportionate, and consistent with the requirements of the HRA.

3. VSS Privacy masking and the Data Protection Act

When considering the use of VSS privacy masking in relation to the seven principles of the Data Protection Act, the following observations can be made:

1. **Lawfulness, fairness, and transparency:** VSS privacy masking must be used in a lawful manner, and individuals must be informed about the use of the technology. VSS operators must have a legal basis for using privacy masking, such as a legitimate interest, and they must provide individuals with clear and transparent information about the use of the technology.

2. **Purpose limitation**: VSS privacy masking must be used only for specified, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes. This means that privacy masking must be used only in areas where individuals have a reasonable expectation of privacy and not used to monitor individuals in areas where they have a reasonable expectation of freedom from surveillance.

3. **Data minimisation:** VSS privacy masking must be limited to what is necessary in relation to the purposes for which it is processed. This means that privacy masking must be used only to the extent necessary to protect individuals' privacy rights and must not obscure or block more than is necessary.

4. **Accuracy:** VSS privacy masking must be applied accurately, and the technique must not obscure or block areas that are not intended to be masked.

5. **Storage limitation:** VSS privacy-masked footage must be kept for no longer than is necessary for the purposes for which it is processed. This means that privacy-masked footage must be stored only for as long as necessary to fulfil the surveillance purpose and deleted or destroyed securely when no longer needed.

6. **Integrity and confidentiality:** VSS privacy-masked footage must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisational measures.

7. **Accountability**: VSS operators must be responsible for and able to demonstrate compliance with these principles. This means that VSS operators must demonstrate that they have taken appropriate steps to ensure compliance with the data protection principles, including using privacy masking.

In summary, the principles of the Data Protection Act are highly relevant to the use of VSS privacy masking, as they ensure that personal data is processed in a fair, lawful, and transparent manner and that the privacy rights of individuals are respected. Compliance with these principles is essential for ensuring that VSS surveillance is proportionate and necessary and respects an individual's right to privacy.

4. Privacy Masking for home private use

The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) set out the legal requirements for processing personal data, including any personal data captured by VSS cameras. These regulations apply to all data controllers, including individuals who use VSS cameras for home (private use).

Under these regulations, individuals who use VSS cameras for home (private use) must comply with certain requirements. For example, they must have a legitimate reason for processing personal data captured by the cameras and ensure that the processing is transparent, fair, and lawful.

Privacy masking can be useful for complying with these regulations when using VSS cameras for home (private use). By obscuring or blurring the faces of individuals captured in the footage, privacy masking can help to protect their privacy and ensure that their data is not processed in a manner that could be considered unlawful or unfair.

However, it is important to note that privacy masking is only a partial solution to compliance with the Data Protection Act 2018 and the GDPR. Individuals who use VSS cameras for home (private use) must also ensure that they provide individuals with access to their data and that the personal data is kept secure and confidential.

Additionally, individuals must ensure that they comply with other requirements of the regulations, such as the requirement to conduct a Data Protection Impact Assessment (DPIA) if the VSS processing is likely to result in a high risk to the rights and freedoms of individuals.

In summary, privacy masking can be a helpful tool for complying with the Data Protection Act 2018 and the GDPR when using VSS cameras for home (private use). However, individuals must ensure that they comply with all regulations and requirements and that their use of VSS cameras is transparent, fair, and lawful.

5. The Freedom of Information Act and the Protection of Freedoms Act

The Freedom of Information Act (FOIA) and the Protection of Freedoms Act (POFA) must be complied with as well as the Surveillance Camera Code of Practice (SCCoP) when using VSS privacy masking in VSS systems.

The POFA regulates public authorities' use of surveillance cameras in England and Wales and requires compliance with the SCCoP. The Code of Practice requires that VSS privacy masking is used proportionately and necessarily, considering the impact on individuals' privacy. It also requires transparency in the use of VSS, including the use of privacy masking, and that clear rules, policies, and procedures are in place for the use of VSS.

Under the FOIA, organisations may be required to disclose VSS footage that includes privacy masking in response to a request for information. However, the FOIA has exemptions for information subject to legal professional privilege, personal data, and information that would prejudice national security, law enforcement, or other public interests.

Under the POFA, organisations must conduct a DPIA before using a surveillance camera system, including video surveillance systems that use privacy masking. The DPIA must assess the impact of the system on individuals' privacy and ensure that it complies with the principles of data protection.

Organisations must also ensure that they have clear policies and procedures for using and disclosing VSS footage, including privacy masking, and that any disclosures comply with the FOIA and other relevant legislation.

In summary, organisations that have obligations under the FOIA and the POFA must comply with both legislation and the SCCoP when using VSS privacy masking in video surveillance systems. It includes conducting a DPIA, ensuring that the use of privacy masking is proportionate and necessary, and having clear policies and procedures for using and disclosing VSS footage that includes privacy masking.

6. Surveillance Camera Commissioner's Code of Practice and Privacy Masking

Code of Practice Principles are particularly relevant to VSS privacy masking.

These include:

Principle 2: Using a surveillance camera system must consider its effect on individuals and their privacy, with regular reviews to ensure its use remains justified. This principle emphasizes the importance of considering the impact of VSS privacy masking on individuals and their privacy. Organisations should regularly review their use of VSS privacy masking to ensure it is still necessary and justifiable.

Principle 5: Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them. This principle highlights the

importance of having clear rules, policies, and procedures for using VSS privacy masking and ensuring that all relevant personnel know them.

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. Such images and information should be deleted once their purposes have been discharged. This principle emphasizes the importance of only retaining VSS footage necessary for its stated purpose. Organisations should not retain VSS footage that includes identifiable individuals who have been obscured by privacy masking once the purpose of the footage has been served.

Principle 7: Access to retained images and information should be restricted, and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or law enforcement purposes. This principle highlights the importance of restricting access to VSS footage, including footage that includes privacy masking. Access should only be granted to authorized personnel with a legitimate need to view the footage.

Principle 9: Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorized access and disclosure. This principle emphasizes the importance of ensuring that VSS footage, including footage that includes privacy masking, is adequately secured against unauthorized access or disclosure. Organisations should take appropriate security measures to protect the privacy of individuals captured in the footage.

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

7. Methods of restricting camera views

A VSS should be designed to limit its coverage so that it does not cover areas or ‘spaces’ 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 should be 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 SCCoP requirements.

Note: With analogue or lower resolution IP cameras, 4-CIF, or digitally based 1MP, 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 ensure that private or public spaces 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.

7.1. Camera positioning

The most effective way to restrict a camera field of view is by careful selection of camera’s position and lens field of view to prevent the camera from overlooking private areas. With fixed cameras this can be relatively straightforward, Still, 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.

7.2. 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:

7.2.1. 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.

7.2.2. 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 from 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 need 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).

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.

8. Artificial Intelligence and Privacy Masking

When using Artificial Intelligence (AI) for privacy masking in video surveillance systems, organisations must comply with the DPA. Under the DPA, organisations must ensure that any personal data captured by VSS cameras is processed legally, fairly, and transparently. It includes ensuring that personal data is processed consistently with the DPA data minimization and purpose limitation principles.

AI can be used to automate the process of privacy masking, making it faster and more efficient than manual masking. AI algorithms can be trained to recognize and identify the areas of the footage that need to be masked and to apply the masking automatically.

One benefit of using AI for privacy masking is that it can help to reduce the risk of human error or bias in the masking process. Human operators may inadvertently miss certain areas that must be masked or apply the masking inconsistently. AI algorithms, on the other hand, can be trained to mask consistently and accurately. However, organisations must ensure that their AI algorithms are accurate and effective in identifying the areas of footage that need to be masked. Additionally, organisations must ensure that they have a legitimate reason for processing personal data captured by the cameras and are transparent about their use of VSS cameras and privacy masking.

Under the DPA, organisations must also keep personal data secure and confidential. It includes ensuring that personal data is not processed in a way that could be considered unlawful or unfair. To address these concerns, organisations using AI for privacy masking should conduct a DPIA to assess the impact of the system on individuals' privacy and ensure that it complies with the principles of data protection.

Overall, using AI for privacy masking can help protect the privacy of individuals captured in VSS footage. However, organisations must ensure that they use AI responsibly and ethically and comply with all relevant laws and regulations, including the DPA. Organisations must also ensure they have a legitimate reason for processing personal data captured by the cameras and are transparent about using VSS cameras and privacy masking.

References

The Surveillance Camera Commissioner's - Surveillance camera code of practice
https://www.gov.uk/government/publications/update-to-surveillance-camera-code

The Information Commissioners Office (ICO) - Video surveillance (including guidance for organisations using VSS)
https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/

The Data Protection Act
https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Human Rights Act
https://www.legislation.gov.uk/ukpga/1998/42/contents

Freedom of Information Act
https://www.legislation.gov.uk/ukpga/2000/36/contents

Protection of Freedoms Act
https://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

Town and Country Planning Order
https://www.legislation.gov.uk/uksi/2015/596/contents

European Convention on Human Rights (ECHR)
https://www.echr.coe.int/Pages/home.aspx?p=basictexts

About **the BSIA**

This guidance has been produced by the Video Surveillance Systems Section of the BSIA.

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.