WHITE PAPER

Privacy in surveillance

Tools and technologies to safeguard privacy

December 2023

AXIS COMMUNICATIONS

Summary

Surveillance solutions must comply with local, regional, or other applicable privacy regulations that place restrictions on the collection of personally identifiable data.

Several tools and technologies exist to help protecting people's privacy in surveillance.

- **Dynamic masking** anonymizes people or vehicles in the video in real time. The analytics application AXIS Live Privacy Shield offers AI-based dynamic masking in selected cameras to detect and mask humans or license plates. It also offers motion-based dynamic masking in all compatible cameras for masking all moving objects.
- **Static masking** hides a selected area by applying a permanent mask on all live and recorded video. This is available as a standard feature in Axis network video products and is ideal for indoor or outdoor scenes where there are fixed areas that you are not allowed to monitor.
- **Video redaction** in video management software (VMS) can be used when you need to export video, for example for a forensic investigation, while safeguarding the privacy of bystanders in the footage.
- **Non-visual surveillance**

  Thermal cameras create images based on heat radiating from objects. Only shapes are captured, without personal details.

  Radars in surveillance provide detection without generating any personally identifiable details.
- **Analytics** based on video or audio can be used to monitor a scene and trigger actions when something stands out. Analytics can also visualize data in dashboards without needing to store any recordings.

The owner of a surveillance system is responsible for ensuring compliance with privacy regulations.

Table of Contents

1 Introduction

There are various options for how to protect privacy in surveillance. You can, for example, block areas in the camera view, mask people in the video, or use non-visual technologies for your surveillance.

This white paper presents the main tools and technologies to address privacy concerns during the capturing, recording, viewing, and exporting of surveillance video.

2 Background

Surveillance in public areas is becoming more accepted as citizens begin to understand how it can increase their safety and security. While privacy has always been a priority in the surveillance industry, people's awareness of their rights has been heightened by initiatives like GDPR (General Data Protection Regulation) in Europe and FISMA (Federal Information Security Management Act) in the US.

In both the public and private spheres, there are rules and regulations from local and regional governments and unions concerning video surveillance and privacy. The regulation is there to protect human rights by safeguarding people's right to privacy. Therefore, it puts in place controls that must be implemented around the capturing, storing, and sharing of video data.

It is always the owner of a surveillance system who is responsible for making sure that their surveillance complies with all applicable local and international privacy regulations. However, manufacturers and vendors can help their customers stay informed on surveillance best practices. This includes how to use the collected data in a correct and ethical way and take the necessary steps to comply with regulations.

3 Masking in video

There are various techniques for hiding selected areas or anonymizing people in surveillance video.

For all types of masking, you can choose between solid color or mosaic (pixeled) masking. Color masking provides the greatest privacy protection while enabling you to see movements. Mosaic masking shows

moving objects or humans in very low resolution and allows you to better distinguish forms by seeing the objects' real colors.

Color masking and mosaic masking.

3.1 Dynamic masking

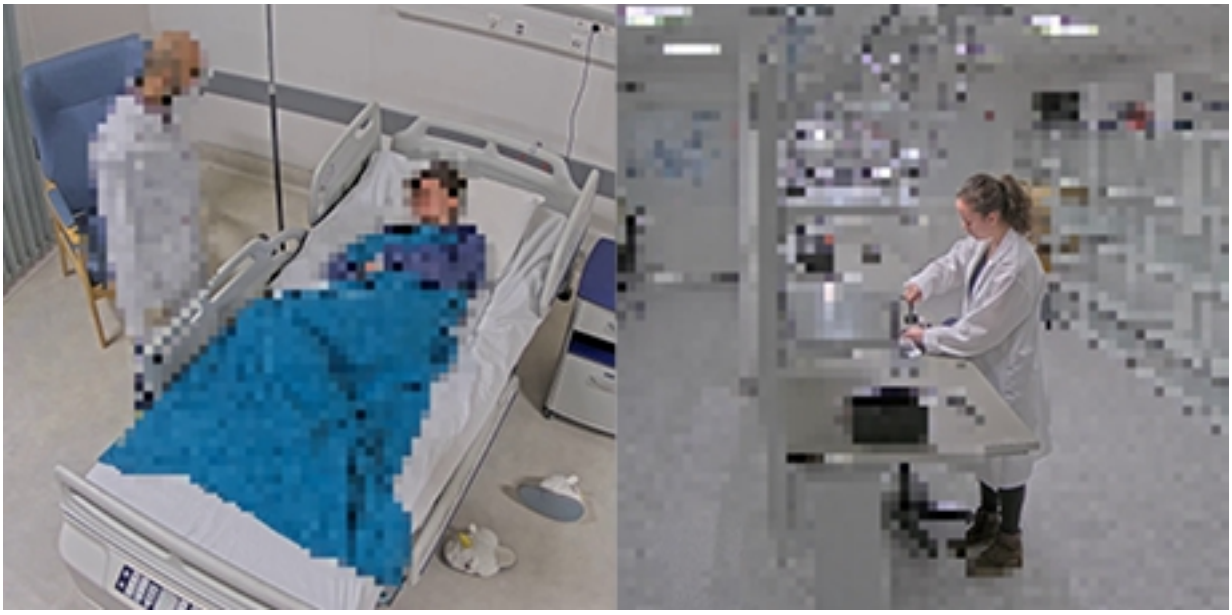
With this technique, video analytics automatically anonymize people in the video. This happens in real-time as the analytics monitor the actions and movements in the scene.

The edge-based analytics application AXIS Live Privacy Shield offers AI-based dynamic masking on visual cameras.

3.1.1 AI-based masking

This is supported in selected cameras that have a deep learning processing unit (DLPU). With AI-based masking, the application analyzes live video to detect humans or license plates. You can choose to mask

either humans (moving and stationary), faces, or license plates. The masking method can also be inverted to mask the background instead.



Masking of humans and masking of the background in AXIS Live Privacy Shield.

AXIS Live Privacy Shield enables AI-based dynamic masking at up to 10 frames per second. It is suitable for near-range indoor and outdoor scenes in places like manufacturing facilities, hospitals, elderly care homes, hotels, schools, offices, and stores.

With AI-based masking, the masking will remain also when persons are still for long periods of time.

3.1.2 Masked and unmasked streams

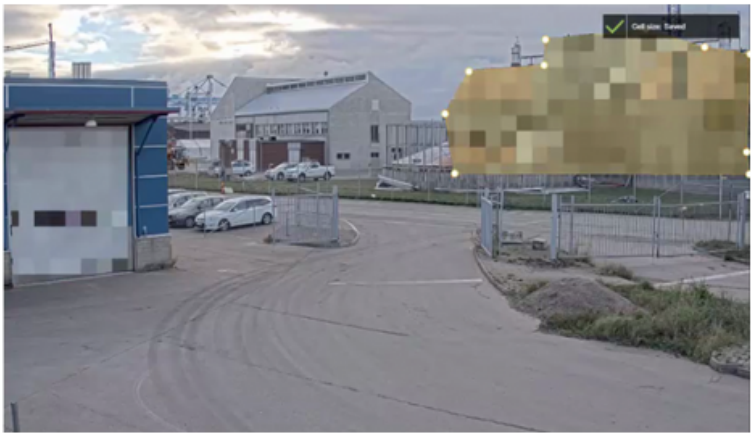
Masking with AXIS Live Privacy Shield is permanent in the sense that it cannot be removed from the video after recording. However, you can choose to have the application deliver both a masked video stream and, simultaneously, a separate stream with no masking. Depending on the VMS, you can configure the access rights of the streams.

This way, you can keep an unmasked stream that only authorized personnel can view. Should the identities of those captured in the footage be crucial to an investigation, there is, then, a way to retrieve that information. Keeping parallel streams not only protects individuals in their right to privacy, but it also covers the surveillance owner's obligations to keep people safe, especially in open, public spaces.

3.2 Static masking

Static privacy masking is ideal for indoor or outdoor scenes where there are fixed areas that you are not allowed to monitor. It hides a selected area by applying a permanent mask (opaque or mosaic) on live and recorded video. With a mosaic mask, the area is shown in very low resolution so you can see activity without personally identifiable details.

Static privacy masking is a standard feature in Axis network video products. It can be combined with the dynamic masking of AXIS Live Privacy Shield.



Static privacy masking using a polygonal mosaic mask to permanently block a building from being monitored.

Masking specific areas to prevent unintended surveillance is especially valuable with PTZ (pan-tilt-zoom) cameras, given their long distance and wide area coverage. In a PTZ camera, static privacy masking is fixed to the camera's coordinate system. As a result, the masking remains in the same area of the scene even as the field of view is changed.

4 Video redaction

When sharing video recordings, you need to comply with any applicable regulations that protect the privacy of bystanders. A video redaction tool in AXIS Camera Station lets you easily mask individuals or areas in a scene that are not of interest to an investigation. You can, for example, mask only selected moving objects or mask all stationary and moving objects except persons of interest.

Note that video redaction cannot be used on live video.

5 Non-visual surveillance

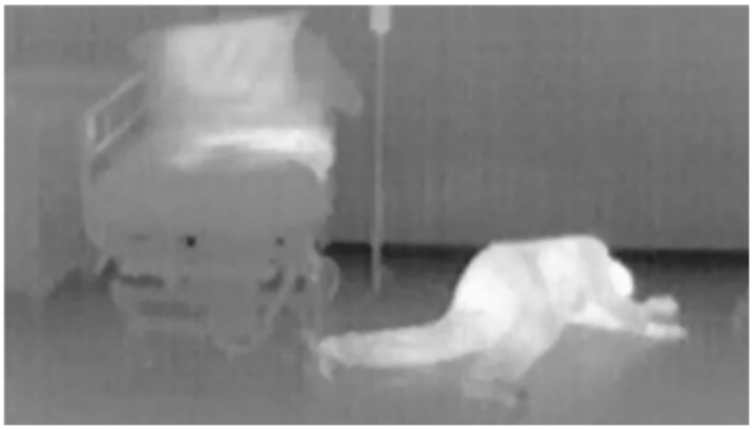
In some cases, privacy in surveillance is best guaranteed using non-visual detectors instead of regular cameras. These solutions work in any weather and any light.

5.1 Thermal imaging

Thermal cameras detect heat instead of visible light. They create an image based on the heat that radiates from objects within the camera field of 'view'. This allows for remote monitoring without collecting personal details. Only shapes – moving or stationary – are captured.

Thermal cameras with embedded motion-detection analytics are useful in environments with high privacy requirements. In locations such as healthcare or senior living facilities, thermal cameras protect personal

privacy while quickly alerting staff to unexpected motion. If a patient falls or needs medical assistance, staff can respond promptly.



Thermal cameras allow for remote monitoring without personally identifiable details.

5.2 Radar

A radar provides surveillance with complete privacy because it uses radar technology instead of video technology.

A radar works by transmitting radio waves and receiving and analyzing the same waves bounced off of objects in its field of detection. Radar technology with analytics detects movement and triggers alarms without collecting personal data. It is ideal for detecting intruders in wide open spaces. The radar can then automatically alert security and activate loudspeakers for deterrence.

5.3 Analytics

Video- and audio analytics can be used to help monitor a scene in real-time and react when something stands out. Analytics generates metadata, which can be used for scene understanding without the need to access the video- or audio streams nor to store the recordings. The data can be visualized in spreadsheets and dashboards, or trigger alarms in real-time. This can help address privacy concerns regarding personal data. Audio analytics can trigger alarms when a microphone picks up sounds associated with, for instance, people shouting, glass breaking, or other anomalous sounds.

6 Data protection

Data protection is out of scope for this paper. However, how video surveillance data is handled is an important aspect of privacy protection. See *www.axis.com/about-axis/cybersecurity* for more information.

T10194474/EN/M2.2/2312

About Axis Communications

Axis enables a smarter and safer world by creating solutions for improving security and business performance. As a network technology company and industry leader, Axis offers solutions in video surveillance, access control, intercom, and audio systems. They are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 4,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden