SECURITY INDUSTRY ASSOCIATION

Data Privacy Code of Practice Video Surveillance

SECURITY INDUSTRY ASSOCIATION

securityindustry.org

Data Privacy Code of Practice – Video Surveillance

Introduction

Video surveillance has been used for security applications since the 1940s and has evolved from analog cameras to IP-based systems that can include analytics and machine-learning capabilities. The rapid growth of networked surveillance, along with the evolution of Internet, cloud and mobile applications, as well as improvements in image quality, have vastly expanded video's ability to deter and detect criminal activity and to provide evidence used to solve crimes and find missing persons.

Emerging analytics technologies add to video's functionalities, with artificial intelligence (AI)-powered systems, for example, able to recognize humans, vehicles, objects and events, then generate alarms that allow users to respond quickly to potential threats. This automation can help to reduce human error resulting from surveillance fatigue, improving alarm accuracy and response. (Privacy guidance specifically related to the use of analytics will be addressed in a future update to this document.)

Given the nature of video surveillance, concerns about potential misuse and invasions of privacy are understandable, and there have, unfortunately, been cases in which a lack of proper controls has led to privacy violations. The Security Industry Association (SIA) Data Privacy Advisory Board has produced this Code of Practice for Video Surveillance ("Code") based on common privacy and security principles to provide manufacturers, integrators and end users with guidance that can be used to inform their development of sound policies and practices that mitigate privacy risks while leveraging the power of video technology

Areas of Responsibility

Manufacturers

For manufacturers, primary responsibilities relate to device and platform default configurations and upkeep, as well as building privacy into the design of hardware and software. Device and platform design and maintenance should include:

- Patching
- Vulnerability communication
- Forced changing of default login credentials
- Role-based access control, multi-factor authentication, encryption, and other data security best practices
- Device security risk considerations and notifications (e.g., trusted platform details)
- Cloud services security and management, if apps are offered
    - Associated security considerations and notifications
- Publicly available and current guidance to secure infrastructure

Integrators

Responsibility for integrators begins with the design and layout of the system. Conducting a privacy impact assessment can identify areas of concern before installation begins. For example, camera viewing areas and the use of analytics software must be addressed in the planning stages. It is critical to establish an appropriate set of default privacy settings, in addition to "hardened" secure settings for cameras and the network, including purpose-specific analytics and viewing/exclusion zones.

Other important areas for integrators to consider include:

- Ongoing privacy and cybersecurity education and training for employees
- Proper authentication of employees on systems and devices
- Requirements, roles and responsibilities, including third-party security
- Nature of systems involved (cloud, on premises, hybrid) and designated privacy and security measures
- Applicable international, federal, state, and local laws and regulations, as well as industry standards, frameworks and best practices
- A service contract that identifies the integrator's privacy and security obligations and risk

End Users

End users are the surveillance system data controllers (in privacy terms). They establish the purpose and justification for the surveillance system as well as its operational scope. When hiring a third-party services provider, the end user should take reasonable steps to ensure that the provider follows all applicable data privacy laws, regulations and best practices and meets the same standards when handling data that the end user has in place for itself. The end user, as data controller, retains the ultimate responsibility to protect sensitive information and respect privacy and should not solely rely on third-party service providers for compliance.

Transparency is a priority, especially regarding the identification of the owner or processor of the data, as it enhances trust. End users must be aware of requirements in jurisdictions in which they operate, because, in many places, there are transparency and notice mandates concerning such information as who is conducting the surveillance, the level of surveillance being conducted, and the risk involved.

Privacy risk factors vary depending on the end user's system and its interactions with individuals. A risk assessment is crucial to determine areas of concern. This assessment should look at the use of video surveillance across the organization and consider business, operational, legal, technical and social aspects. It should begin by addressing the most basic questions, such as identifying the purpose of the surveillance, who or what is being surveilled, and what the justification is.

The following is a non-exhaustive set of questions that operators in several sectors can use to begin to determine potential privacy risks. Security system operators are the systems administrators for the data controllers who authorized the surveillance.

Corporate security

- How is video being used?
- Can data subjects be identified?
- Are analytics being used?
- Is there notice of surveillance before it takes place?
- Is there an opt-in option? Or opt-out? Or right to be forgotten?
- What are the retention times? How do these compare to legal requirements, if there are any?

Healthcare facilities

- Are there HIPAA compliance requirements?
- Are there protected health information (PHI) implications?

Education

- Are there Family Educational Rights and Privacy Act (FERPA) considerations?
- Is facial recognition being used for attendance?
- Have parental concerns been considered and addressed?

Marketing

- What levels of transparency and notice are in place?
- Are there PII concerns with how the video is collected, used and stored?
- Are data subjects being identified? If so, is this necessary/appropriate?

Public/Government/Law Enforcement

- Who/what area is being surveilled and why?
- Is artificial intelligence (AI) or another automated technology being used?
- Is appropriate notice/signage in place in place?

Code Principles

This Code of Practice is based on core privacy and security principles as they apply to the manufacture, deployment and use of video surveillance systems. As with any technology-based security system and the products developed for such systems, conducting a privacy impact assessment (PIA) can establish a baseline for appropriate privacy practices. This begins with the design phase and continues through to deployment and use.

A PIA analyzes how information is collected, used, shared, maintained and retained and identifies the operational requirements. (These requirements extend beyond compliance as they also drive governance and resulting policy.) Further, a PIA can identify areas in which privacy violations would occur if surveillance were used, with some obvious cases being surveillance in

a restroom and inadvertent capture of identity and payment cards. One should also be aware of the integration of video surveillance with identity management and physical access control systems.

In addition to conducting a PIA, implementing the following principles can further improve the privacy practices of manufacturers, integrators and end users.

Privacy by Design

Privacy by design approaches privacy from a proactive rather than reactive perspective. In practice, this means anticipating and preventing breaches before they occur and recognizing privacy rights and enabling their exercise. For manufacturers, this means approaching product design from a privacy standpoint. For integrators, it means designing and installing video surveillance systems that incorporate privacy principles in their use and maintenance. Organizations adopting privacy by design will have to make privacy a priority in determining default settings and must keep all stakeholders informed of their privacy practices and any changes that are made to them.

Regular Review

Establishing consistent and regular review and audit processes will help to ensure compliance with legal and regulatory requirements and industry standards and best practices. These will need to be updated from time to time as circumstances or technological advancements dictate. The review should include all stakeholders, including individuals and third parties that may be affected.

Transparency and Notification

- Inform consumers and employees that cameras are in use
- Provide information regarding the data captured and how it will be used and limit uses to those for which there is legal justification
- Share data retention information (e.g., how long information will be stored, how it will be deleted)
- Include a point of contact for complaints or further information

Purpose Limitation

Use video surveillance systems for a specified purpose that meets an identified and pressing legitimate need

Data Minimization

Collect only that video that is necessary for the intended purpose

Data Accuracy

Data controllers are responsible for the accuracy of the data. Make sure that the metadata concerning location, date, time and other factors are accurate. In some cases, the data accuracy needs to meet evidentiary requirements. If analyzing data and comparing it to a reference database, ensure that the database is accurate and kept current. For video surveillance purposes, manipulating video images requires notation and should be avoided unless absolutely necessary.

Data Storage Limits

Only store video footage for as long as is reasonably necessary or required by law or regulation.

Integrity, Confidentiality and Security

Implement appropriate processes, policies, and procedures to process and store data in a secure manner. This could include the use of digital signatures and watermarking to prevent modification as well as other cryptographic techniques, such as encryption during transmission and storage. Regularly review processes, policies and procedures to protect against unauthorized access or use.

Data Access

Restrict access to data and retained images. Clearly define rules stating who has access and when and for what purpose access may be granted.

Selected Glossary

Data Controller – Determines the purposes for which, and the means by which, personal data is collected and processed and the related policies; for the purposes of this Code, the end user typically is the data controller

Facial Recognition – A software application found in video surveillance systems that can compare a human face in an image to a database of faces and identify matches

Integrator – Designs, installs and manages security solutions (sometimes through third parties) to protect people, data and assets

Multi-factor authentication (MFA) – An electronic authentication method that grants a user access to a website, application or facility only after they have successfully presented two or more pieces of evidence to prove they are who they say they are; this typically includes something they know such as a password, something they have such as a token, and/or something they are such as a fingerprint

Patching – A change to a computer program or its supporting data that updates, fixes or improves the program, often by addressing an identified vulnerability

Personally identifiable information (PII) – Information that can be used to identify an individual, either by itself or when combined with other information

Privacy impact assessment (PIA) – A tool that can be used to gauge risk by examining the way projects, systems, programs, products and services collect and use data; a PIA needs to take into consideration the operational requirements that a Data Controller must meet

Protected health information (PHI) – medical and health information that can be linked to an individual

Disclaimer: *The information provided in this Code does not, and is not intended to, constitute legal advice. All information is for general informational purposes only. Readers of this Code should contact their attorney to obtain advice with respect to particular legal matters. No reader of this Code should act or refrain from acting on the basis of the information in this Code without first seeking legal advice from counsel in the relevant jurisdiction. The content of this Code is provided "as is"; no representations are made that the content is error-free.*

SECURITY INDUSTRY ASSOCIATION

securityindustry.org