SECURITY INDUSTRY ASSOCIATION

# PRIVACY FRAMEWORK

Members of the Security Industry Association (SIA) share the public's concern about the impact of certain technologies upon individual privacy. SIA has a long history of building public interest community, government, and industry support for voluntary best practices that will strike a balance between legitimate privacy concerns and appropriate uses of electronic physical security technologies. In 2000, SIA and the International Association of Chiefs of Police and the National Sheriffs' Association completed years of collaboration and adopted the "CCTV for Public Safety and Community Policing Guideline." The guideline builds upon a vast reservoir of public safety and legal knowledge and experience and serves as a "How To…" document for those law enforcement and private sector entities seeking to implement a CCTV for Public Safety program.

Over the past several years, there has been an increasing level of state legislative activity that is intended to severely limit or restrict the use of electronic physical security technologies. Such legislative proposals have been introduced in response to well-intentioned concerns about the use of these technologies. SIA has been a leading voice before certain state legislatures in seeking to reverse this trend and defeat ill-advised proposals that would deprive state and local governments from accessing the technologies they need to prevent violent crime and terrorist attack.

As an active participant in these legislative debates, SIA recognizes that government programs that seek to address a user's privacy can have a profound and costly effect upon the use of biometrics, CCTV, RFID, and other security technologies used by end-users. Overly restrictive government privacy policies can lead to excessive litigation, prevent the delivery of cutting-edge security solutions to end-users, and impose unnecessary delays in the allocation of grant funds for critical infrastructure protection projects at our nation's ports, transit systems, schools and universities, and other essential facilities. SIA members know all too well how changes in technology occur much faster than legislatures and policy-makers can address those changes.

For these reasons, SIA members wish to continue the electronic physical security industry's positive contributions to the debate over privacy and security by professing their commitment to the following privacy principles. These privacy principles are intended to complement, rather than supplant, past and ongoing efforts by SIA and its partners to develop best practices and/or guidelines for the use of electronic security technologies. The principles should not be interpreted as negating the "CCTV for Public Safety and Community Policing Guideline" or any modification to that document. Instead, these principles are part of SIA's overall response to the influence of privacy within government policy and upon businesses.

## PURPOSE

This privacy framework has three intended purposes:

- to serve as a guideline for manufacturers, integrators, and distributors of electronic security technologies, including but not limited to biometrics, video safety systems, and RFID;
- to provide information to government policymakers about how the electronic security industry protects privacy when collecting, securing, and storing personally identifiable information; and
- to help educate end-users and customers about how privacy challenges associated with the use of these technologies are being met.

## SIA PRIVACY PRINCIPLES:

SIA members are committed to developing and communicating best practices and comprehensive privacy policies to clearly explain the use, storage, and handling of personally identifiable information and how privacy issues are addressed.

SIA and its member companies support the following guidelines in the deployment of electronic physical security systems:

1. Privacy impact assessments undertaken by system owners and managers to analyze how personally identifiable information collected is stored (and for how long), protected, shared, managed, and disposed of.
2. An assessment of any legal compliance regulations that might affect the system, data and end-users (i.e., Sarbanes-Oxley Act, Health Information Portability and Accountability Act, etc.).
3. The implementation of privacy-enhancing solutions, when possible, during the design phase of electronic security products, services or systems for access control applications with such solutions commensurate with the level of risk.
4. Adequate protection and security of the database where any personally identifiable information collected for use in an access control system is stored.
5. Adequate protection and security of any data shared between systems or components commensurate with degree of possible exposure of said data.
6. Notification given by the employer to individual users about the purposes and uses for collecting data for the access control system and how that data may be used in the future. If employers are using the system to monitor employees, informing employees of the intent to monitor.
7. Limits on access to personally identifiable information stored in an access control system within an organization based on a "need to know."
8. Adoption of a security-breach notification plan by end-user customers that includes:
   - A mitigation procedure.
   - Fast and dependable means of determining whether notification is required to individuals with personally identifiable information in the database.
9. Immediate responsive action if a privacy breach does occur.
10. Regular collaboration with end-users of electronic security systems to help ensure privacy and security compliance.
11. A retention policy for personally identifiable information:
    - If video, a time period for retaining (storing) video for both non-incident and incident video.
    - If PACS, a policy that dictates when personally identifiable information is destroyed after an individual is no longer authorized within the system.
12. A procedure to ensure that personally identifiable information in item 11 above is destroyed completely.