# SIA Principles for the Responsible and Effective Use of Facial Recognition Technology

## Table of Contents

SECURITY INDUSTRY ASSOCIATION

securityindustry.org

# Introduction

The Security Industry Association (SIA) is a nonprofit trade association representing more than 1,100 businesses providing a broad range of security products and services in the United States and internationally. Our members include many of the leading developers of facial recognition technology; companies offering products that incorporate this technology in a variety of identity, security and public safety applications; and installers and integrators of these systems.

**Our Values.** SIA believes all technology products, including facial recognition, must only be used for purposes that are lawful, ethical and nondiscriminatory. As demonstrated throughout its 30+-year history of development, facial recognition technology offers tremendous benefits to society when used effectively and responsibly. Industry has a duty to ensure that advanced technologies, particularly those enabled by artificial intelligence and machine learning, are used in a responsible manner consistent with our values and with appropriate safeguards.

**The Benefits of Facial Recognition.** The benefits of facial recognition are proven and growing, through a wide range of vastly different applications. For example, in the United States, the technology has been used for more than a decade to detect identity fraud that fuels other criminal activity. It also been used to help find and rescue human trafficking victims, thwart potential terrorist attacks, solve hate crimes and crack cold cases. More information about these successes of facial recognition can be found on SIA's website.

As a means of digital identification, facial recognition can be a vital enabler for commerce by improving security, protecting identity, safeguarding our personal devices and enabling touchless access and a seamless travel experience. In the security field, facial recognition is critical, as it enhances the effectiveness of security and life safety systems to help our customers keep their facilities, employees and patrons safe.

**Our Principles.** We have committed to the following principles to be used in the development and deployment of facial recognition technology. We believe that that these principles should apply to implementation of facial recognition tools across safety and security applications in both public- and private-sector settings and should be reflected in development of any organizational or public policies addressing these uses of the technology.

## Core Principles

**Transparency.** Transparency is the bedrock that governs the use of facial recognition technology for both commercial and government use. Transparency is critical to security and privacy, as it helps build and maintain public trust. It should be clear when and for what purpose the technology is used as well as which processes and procedures govern the collection, processing, storage, use and transfer of related data. Importantly, transparency should ensure that every application of the technology is subject to a policy set by the implementing organization, which governs how the technology is to be used.

**Clear and Defined Purpose.** Organizations using facial recognition must specifically identify their purposes for using the technology; they must understand the capabilities and limitations of the systems they intend to use and ensure that the technology is selected and configured appropriately for that purpose. Similarity thresholds and other performance settings should be highly tailored according to the intended use.

Facial recognition is an image comparison technology that provides a similarity score for one (or many) facial images compared to another, just like other biometric technologies that compare physical traits. No biometric technology is 100 percent accurate, and performance can vary considerably across different accuracy metrics and between developers. The performance metrics that matter, and score thresholds for indicating a potential match, are not the same for all applications that vary by user impact, database size and other factors.

**Using Accurate Technology.** Organizations must strive to use the highest-performing facial recognition technology for a given application, with accuracy validated using sound methods, such as through the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) program, the global gold standard for scientific, independent evaluations of facial recognition algorithm performance. Additionally, the NIST FRVT program measures the differences across demographic groups, which is a critical consideration for buyers of these systems.

Both developers and end users have a responsibility to minimize any negative effects that could result from variability in technology performance though proper design, selection and configuration of the technology, as well as policies and procedures addressing human elements of the application. Additionally, providers have a responsibility to provide training – and retraining, as appropriate – for technology buyers to ensure that they are using these systems in appropriate ways.

**Human Oversight.** Human oversight and review are critical factors in identification processes aided by facial recognition technology. While facial recognition software automates image comparison and matching, it must not automate decision making without human oversight at a level appropriate to the application. Some applications require peer review of search results and conclusions.

**Nondiscrimination.** Facial recognition should only be used in ways and for purposes that are nondiscriminatory. There are legitimate concerns that some applications of facial recognition technology might negatively impact minorities. The purpose of using biometric technologies in safety and security applications is ultimately to better protect people from harm. Any significant bias in technology performance makes it harder to achieve this goal. Accordingly, the security industry must recognize this risk and prioritize continual improvement of these tools to provide technology that is suitably effective and accurate across all types of uses, deployment settings and demographic characteristics.

The December 2019 NIST Demographic Effects report provides a comprehensive snapshot of the progress industry is making. The report found that the highest-performing technologies – including those used in key U.S. public-sector programs – had "undetectable" differences in performance across given demographic groups and that the performance of most others was much more consistent than had been widely reported in the media and several nonscientific tests.

**Data Security.** Facial recognition data transmission, storage and processing should be optimized to ensure privacy and security using encryption and other cybersecurity and privacy best practices that protect biometric data. Solutions should follow a distributed data approach by limiting biometric data stored in central repositories and storing this data in the form of encrypted digital templates rather than original images. Each developer measures and records templates differently, providing an additional layer of security by making this data useless if compromised, either for identification or as a credential outside of the system that created it. As with processing algorithms, advances are being made in data security with techniques such as homomorphic encryption that allows processing without decrypting data.

**Privacy by Design.** Privacy protections are critical in deployment of facial recognition technology, as, in most cases, these tools create a link between a person's facial appearance and personally identifiable information (PII). Facial recognition systems should be designed to facilitate compliance with current and emerging data privacy laws and support privacy practices and ongoing system maintenance. Design, development and testing of the technology should comply with Fair Information Practice Principles and relevant principles derived from these, such as SIA's Privacy Framework.

Organizations using facial recognition systems should ensure a culture of accountability internally and across third-party service providers and business partners. To this end, government users should establish and publicly disclose governance policies that guide their use of such systems and provide an opportunity for feedback.

**Training and Education.** It is critical that users of facial recognition technology know how to configure and maintain facial recognition technology, consistent with their policies. Additionally, sellers of this technology should provide buyers, installers and operators with training on how to achieve the most accurate and nonbiased results and commit to doing so on an ongoing basis.

**Ethical Acquisition.** Given the unique needs of many public-sector applications, government entities should only purchase facial recognition technologies that perform highly overall and across demographic groups and are validated using sound, scientific methods. Any organization fielding facial recognition technology should also carefully consider their technology providers and refrain from working with companies and/or products that are implicated in human rights abuses or for other purposes that do not meet the standard of lawful, ethical and nondiscriminatory use.

**Targeted Public Policy.** Addressing public concerns about current and potential applications of this technology can be fully accomplished through policies promoting transparency, proper procedures and thorough oversight, which allows the approach to facial recognition technology to be adapted as appropriate and as technology evolves. Prescriptive legislation or regulation are the least flexible ways to provide governance over this technology.

Clear and effective policy must distinguish facial recognition from other technologies with which it is often erroneously confused, like facial detection, analysis counting or tracking – which may not involve specific, individual identities. Facial recognition, as properly defined by NIST and understood in the industry, is used for two distinctly different types of applications: **verification**, which helps determine that a person is who they claim to be, and **identification**, which generally helps human analysts determine whether an image of an unknown person matches an identity in a specific database.

It is unlikely all the scenarios could be adequately addressed by a one-size-fits-all legislative framework. Development of any policy on facial recognition must take a risk-based and use case-specific approach. Blanket moratoriums and bans shutter both proven current uses and potential future benefits across many uses. National polls have found that fewer than one in five Americans would support strict limits if it came at the expense of public safety, and more than half of Americans trust law enforcement to use the technology responsibly.

Above all, policies must be informed by a clear understanding of both the advantages and the risks, supported by sound information and honest public dialogue.

## Public-Sector Applications

Public-sector uses of facial recognition technology are extremely varied, including identity verification, security and law enforcement investigative applications. As public-sector uses are more likely to be part of processes with consequential outcomes, it is especially important for transparency and sound policies to accompany government applications, which can be accomplished through the following.

**Legitimate Public Interest Purpose.** Government entities should only use facial recognition technology for legitimate, lawful and well-defined purposes, consistent with our constitutional framework, laws and regulations.

**Clear Use Policies.** Every public-sector implementation of facial recognition technology should be accompanied by policies written in a clear and understandable manner, with a point of contact for inquiries. For search-based identification applications, each policy should describe who is authorized to use a system under what circumstances and outline the role of human review, any privacy impact assessments and rules governing the retention of files contained in the image repository and search images. We encourage government entities to make a public version of such policies available for increased transparency.

**Acquisition Transparency & Integrity.** The public should be informed about what officials are buying and the potential impacts and consequences of those purchase decisions. The following can help accomplish this.

- Establish public comment periods prior to acquisition to bolster public trust and ensure that acquisition decisions reflect public priorities.
- Allow agency-applicable privacy and civil liberties personnel to participate in the acquisition process and decision making.
- Require a competitive acquisition bidding process to ensure that public-sector agencies invest in highly developed facial recognition solutions.
- Limit procurement from any entities that have supported human rights or civil rights abuses and/or that otherwise pose cybersecurity or national security risks.

**Accountability, Accuracy and Security.**

- **Operational requirements** – Officials operating facial recognition technologies should follow best-practice operational guidance from the technology providers and public-sector experts.
- **Testing/performance assessments** – Government entities should only purchase facial recognition and facial analysis technologies that perform highly overall

and across demographic groups. Facial recognition procurement decisions should be based on reported test results from established third-party government testing authorities, such as the NIST FRVT program. Expanding FRVT to allow testing of cloud-based facial recognition would further public-sector accountability and transparency by benchmarking a larger field of available technology.

- **Standards** – Officials should ensure that any procured facial recognition technologies adhere to applicable industry procedural, performance and technical standards, such as those provided by the Facial Identification Scientific Working Group and the Organization of Scientific Area Committees for Forensic Science Facial Identification Subcommittee.

**Accountability Mechanisms**. Such mechanisms provide additional assurances that policies established are being followed and can take many forms, not limited to internal or third-party audits of system design and configuration, personnel usage, operational performance testing and other means. Accountability is critical to verify adherence to the requirements established.

**Operator Training**. Organizations should provide training on the appropriate use of the technology for all personnel who interface with facial recognition systems and provide more in-depth training for those that have access to, configure and maintain those systems to ensure accurate and unbiased operations given the use case and deployment conditions. In addition, we urge all technology providers to offer related training supporting this objective on a regular basis.

## Law Enforcement Use

In all known uses by U.S. law enforcement agencies, a facial recognition search is just one part of an investigative process, which requires a human analyst to confirm whether any potentially matching photo provided from the database queried likely matches a submitted image. Still, facial recognition matches are leads only – not positive identification, which requires additional steps to determine whether the person in an image is the person whose identity is in question. Importantly, as law enforcement agencies using the technology have repeatedly stated, *the technology itself cannot be used to convict a person of a crime*, because it does not establish probable cause to even arrest a person or obtain a search warrant.

As NIST has documented, facial recognition combined with human analysis is more accurate than human recognition alone. Without the technology, we are left with far less efficient and less accurate manual processes of image comparison, which are potentially subject to greater human bias. Additionally, eyewitness identifications in criminal investigations are notoriously prone to error; according to the Innocence Project, mistaken eyewitness identifications have been the key factor in 71 percent of wrongful convictions in the United States later overturned. The decade-plus operating history by law enforcement agencies in the U.S. has demonstrated the value of facial recognition in achieving objectives that are in the public interest, including reducing human error and eyewitness misidentification, quickly eliminating innocent persons as potential offenders during investigations and cracking cold cases.

Ensuring adherence to thorough and appropriate use policies will help ensure continued success. The U.S. Department of Justice's Face Recognition Policy Development template offers a comprehensive inventory of good practices to consider when developing a law enforcement agency facial recognition policy. Additionally, the following principles should be applied to law enforcement use of facial recognition technology, reflecting best practices from agencies around the country.

**Agency Use Policies**. All law enforcement usage of facial recognition technology should be accompanied by clear use policies for each type of application that articulate who is authorized to use the technology, under what circumstances and with what level of human oversight and should reinforce that constitutional limitations apply to facial recognition deployments. Law enforcement agencies should make public versions of such policies available for increased transparency.

**Legitimate Law Enforcement Purpose**. Law enforcement should only use facial recognition in circumstances where there is a legitimate law enforcement purpose and justification, such as:

- When there is reasonable suspicion the subject has committed or is committing a crime.
- To help identify an individual that may be a missing person, crime victim or witness to criminal activity.
- To help identify a deceased person.
- To help identify a person who is incapacitated or otherwise unable to identify themselves.
- To help identify an individual who is under arrest who does not have or provide valid identification.
- To help mitigate an imminent threat to public safety or significant threat to life, including acts of terrorism as defined by the Homeland Security Act of 2002.

Accordingly, law enforcement should never use the technology in the following ways:

- As positive identification of an individual, or as the sole basis for an arrest.
- To conduct mass surveillance, which means the use of facial recognition tools to search facial images of persons in a public place when there is no reasonable suspicion to believe that they have engaged in criminal activity.
- In violation of an individual's constitutional rights under the First, Fourth and Fourteenth Amendments, such as surveillance based solely on:
    - Religious, political or social views or activities.
    - Participation in lawful events.
    - The race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation or other classification protected by law against discrimination.

  Special consideration must be given to use in public spaces, especially in the context of First Amendment protected activities. By policy, law enforcement should not use facial recognition on an image of an individual participating in such events or possessing characteristics in the categories noted above, unless a reasonable suspicion is held that the individual has committed or is committing crime.
- For any other purpose that is not a legitimate law enforcement purpose.

**Operator Training**. Law enforcement agencies should require all users of facial recognition technology to receive mandatory training that includes but is not limited to the history of the technology, forensic face comparison, the purpose of policy, agency standard operating procedures, data protection, video image extraction techniques, image enhancement regulations, acceptable use, prohibited use and the impact and consequences of policy violations. In addition to training related to using facial recognition technology, investigators and analysts should undergo rigorous training to reduce any implicit bias.

The purpose of facial recognition technology is to help achieve an accurate match – bias in any form, whether human or technological, makes it harder to achieve that goal.

**Images and Adjustments.** Any substantive manipulation of an image for use in a facial recognition system must be documented, preserve the original image, serve the purpose of accuracy enhancement and be consistent with the technology provider's intended use and training. Additionally, sketches, other manually-produced images and look-alike photos are not suitable for use in identification processes aided by facial recognition.

## Private-Sector Applications

In the private sector, facial recognition provides an option to securely and conveniently prove an individual's identity in order to enter a venue, board a plane, perform remote online transactions and access personalized experiences – all while reducing the need to show documents containing PII. In airports across the country, the technology is giving passengers the option to quickly and seamlessly pass from the curbside to their airplane seats in a sanitary manner and, in some instances, without removing their identification or boarding passes from their pockets.

Specific to what the security industry provides, facial recognition is also enabling businesses to better protect their employees, customers and property. Facial recognition can provide additional security for facility access control, typically to augment other access credentials such as keys or cards, which can be shared, stolen or simply lost; in large buildings, this can dramatically increase the speed of entry, streamline elevator use and even enable building automation for customized occupant experience. Buildings with high security needs can utilize a photograph along with another credential to easily add multifactor authentication. The technology also gives businesses the ability to alert staff to a potentially dangerous situation, where an unauthorized person attempts to enter a property.

The following principles should generally guide private-sector uses of facial recognition technology.

**Legitimate Business Purpose**. Facial recognition technology should be used for legitimate, well-defined purposes relevant to the purpose of the organization, consistent with the rights of individuals.

**Use Limitation**. Organizations should ensure access to a facial recognition system is limited to the minimum number of authorized individuals for authorized purposes.

**Data Protection**. Facial recognition data should be obtained, used and stored only for legitimate business purpose, and linkage with PII should be minimized. Data should be protected according to information security and privacy best practices and any requirements in the organization's jurisdiction pertaining to the handling of PII or other types of consumer data. Facial recognition data should be retained only for so long as needed for a legitimate business purpose, then destroyed.

**Reasonable Notice.** Organizations should provide reasonable notice to individuals who, by continuing a course of action, will make their image subject to facial recognition analysis by the organization, unless public safety considerations make this infeasible.

**Voluntary Applications Should be Consent-Based.** Enrollment in facial recognition applications that offer convenience or other commercial benefits should be based on prior consumer consent.

**Clear Criteria for Safety/Security Applications.** Enrollment of an image in a facial recognition system for physical security, safety, fraud prevention or asset protection purposes should be guided by easy-to-understand written policies governing the criteria and human review process by which the enrollment is approved. Such implementations must also respect the reasonable expectations of privacy held by customers and individuals whose images or information are captured by security devices.

**Provide Redress Mechanisms.** Organizations using facial recognition technology should provide a process for individuals to resolve any problems arising from their collected information. It may also require the ability to make a request for deletion/destruction of their facial recognition data.

**Uniform Treatment of Biometric Data.** Biometric data used by facial recognition technology is not fundamentally different than other biometric data. As such, all types of biometric data should be subject to the same usage obligation under any consumer data privacy policies at the municipal, state or federal level.