

John Long

From: Joe Hoellerer <JHoellerer@securityindustry.org>
Sent: Monday, June 24, 2019 11:17 AM
To: City Council
Cc: City Clerk Contact
Subject: SIA's Comments on Ordinance 208142: Facial Recognition
Attachments: Face Facts Dispelling Common Myths Associated with Facial Recognition Technology.pdf

Good Morning Members of the Somerville City Council:

On behalf of the Security Industry Association (SIA) and in advance of tonight's Legislative Matters committee hearing, please include the following documents into the official record. The first is an attachment with a policy paper entitled, *Face Facts: Myths Associated with Facial Recognition Technology*. The second, is a [link](#) to a recent WIRED article entitled, *How Facial Recognition Technology is Fighting Child Sex Trafficking*.

We strongly encourage members of the City Council to review each comment and reconsider advancing Ordinance 208142. Please let me know if SIA could serve as a resource to your offices in the future.

Best,

Joseph Hoellerer
Senior Manager – Government Relations
Security Industry Association (SIA)
8405 Colesville Road, Suite 500
Silver Spring, MD 20910
jhoellerer@securityindustry.org
(p) 301.804.4714
www.securityindustry.org

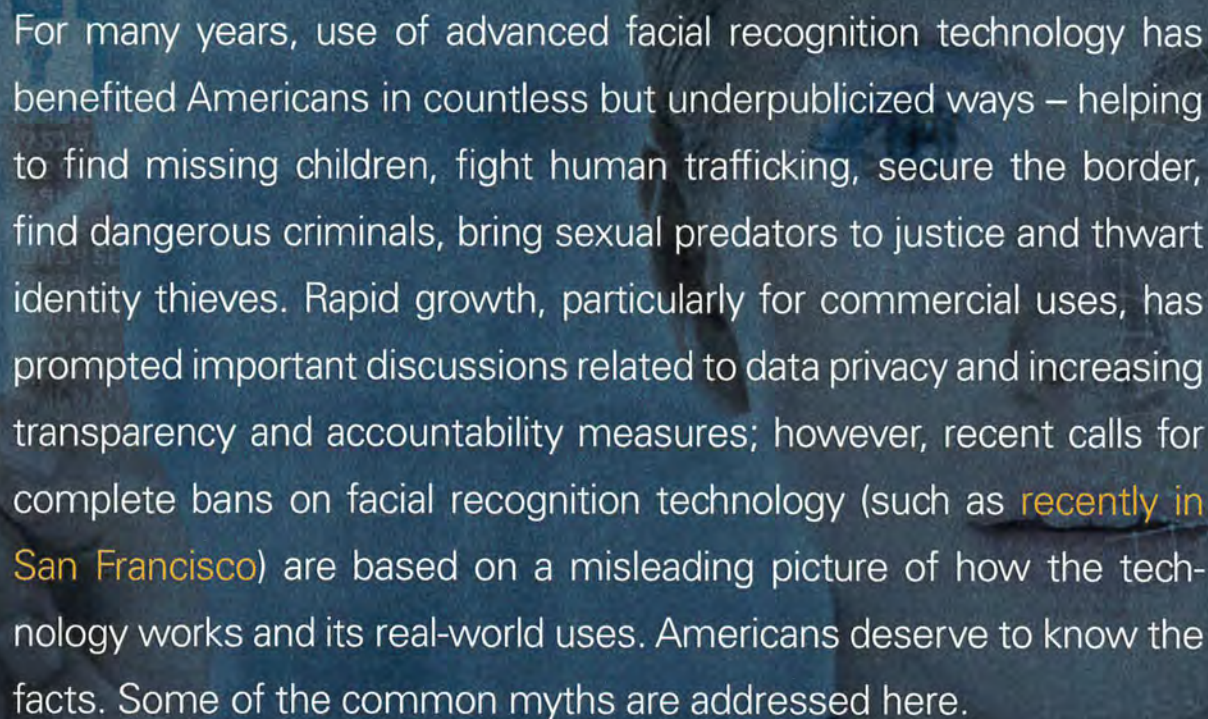
Confidentiality Note: This message and any attachments may contain legally privileged and/or confidential information. Any unauthorized disclosure, use or dissemination of this e-mail message or its contents, either in whole or in part, is prohibited. The contents of this email or for the intended recipient and are not meant to be relied upon by anyone else. If you are not the intended recipient of this e-mail message, kindly notify the sender and then destroy it.



Face Facts: Dispelling Common

MYTHS

Associated With Facial
Recognition Technology



For many years, use of advanced facial recognition technology has benefited Americans in countless but underpublicized ways – helping to find missing children, fight human trafficking, secure the border, find dangerous criminals, bring sexual predators to justice and thwart identity thieves. Rapid growth, particularly for commercial uses, has prompted important discussions related to data privacy and increasing transparency and accountability measures; however, recent calls for complete bans on facial recognition technology (such as recently in San Francisco) are based on a misleading picture of how the technology works and its real-world uses. Americans deserve to know the facts. Some of the common myths are addressed here.

What Is Happening?

Advances in computing power combined with rapid improvements in the quality of photo and video technology developed by the security industry over the last 15 years have allowed facial recognition technology to develop and mature. Today, this proven technology is used in many ways to improve privacy and security through more accurate identity authentication, and benefit consumers and society. Facial recognition is critical to the security field because it enhances capabilities of solutions like video security, access control and identity management systems for the protection of people, property and information.

At the same time, there are many misconceptions about facial recognition technology in the U.S., driven by not only TV and movies but also biased media narratives and provocative reports not supported by facts and designed to create fear and mistrust in the technology, the industry and various public safety agencies.

There is often a perception of a false choice between privacy and security that distorts the actual potential trade-offs. For example, in verification, facial recognition is used mostly in cases where individuals have consented or are required to prove their identities; as a result, making existing identity verification processes faster and more accurate has no negative impact on privacy.

These flawed narratives also often cite reported uses of technology in other nations that would never be acceptable in the U.S. or permitted within its law and policy framework. To be clear, any technology tool could be misused by those that wield it. The Security Industry Association (SIA) believes all technology products, including facial recognition, must only be used for purposes that are lawful, ethical and non-discriminatory. Advanced image and video analysis can and should be a catalyst for good in the world.

How Does the Technology Work?

Fundamentally, facial recognition technology performs comparisons of digital photos. (Note: Facial recognition is distinct from other types of analytics, which include object identification and categorization, as well as face detection and categorization, which are not designed to help identify an individual.) Each photo is converted to a unique numerical value (called a faceprint or template) based on measurements of facial features and associated with an identity in a database. Comparison images are captured either by taking photos or extracting them from video. These photos are similarly converted to numerical values, then compared using an algorithm. This process results in a similarity score based on the probability that the photos are of the same person.

Facial recognition has two distinctly different configurations that are further adapted and tuned for various purposes in different scenarios.

- **Authentication/Verification – helps verify a person is who they claim to be.**

In this case, the system checks a submitted photo against an existing template to verify that it is the same person, hence the term one-to-one (or 1:1) matching. Performance is measured by the verification rate – the rate at which the system successfully verifies that a pair of images are of the same person based on the similarity score.

The primary benefit of this configuration is providing an additional factor for authenticating an individual and greater assurance that an individual is who they are claiming to be. This configuration is applicable to banking, electronic payment, personal electronic device unlocking, employee time and attendance, secure building or door access for employees and guests, air traveler entry-exit and other border crossing systems, passports, preventing identity theft and fraud and other uses.

- **Identification/Discovery – helps determine who a person is.**

In this case, the system compares a photo of an

unknown person to a set of existing templates in a data set that can range from large databases to a small watchlist. This is called one to many (or 1:N) matching. Searches of the data set using an algorithm return a candidate photo or group of candidate photos based on the similarity score. If there are no close potential matches, none are returned. Performance is measured by the accuracy rate – the rate at which the matching image is returned as a candidate – or, conversely, the failure rate – the rate at which a matching image is not returned despite being in the data set.

The primary benefit of this configuration is that it automates the initial step of sifting through large numbers of photos, where it is more efficient, objective and accurate than human analysts performing this same *initial* step manually prior to reviewing potential matches.

Because there are so many uses of facial recognition technology, accuracy thresholds are highly configurable and set based on the specific use case and needs of the user – for example, by returning results above a 90% similarity score. There are legitimate reasons why a user would need to set a lower accuracy threshold to return more candidates for human review. Having a low-quality comparison image or one in which expressions or various other factors can affect the threshold means the matching photo could have a lower similarity score than other comparison images in a data set. A lower threshold would also be helpful, for example, in searching for someone who went missing as a child and would be much older in current photos.

It is critical to understand that for identification/discovery, “false positive” results are inevitable due to the simple fact that similarity scores are based on probability. Developers have configured systems to continuously learn and improve, so the prevalence of false positives can be reduced over time. Unlike with a medical test, for example, the fact that a system may frequently return false positive match candidates doesn’t mean facial recognition technology is flawed; it does, however, highlight the importance of setting the appropriate similarity threshold for a given use – the right tool for the right job – and the necessity of human review and confirmation where match determinations could have significant implications, such as in law enforcement investigations.

Why Is There Confusion About Facial Recognition?

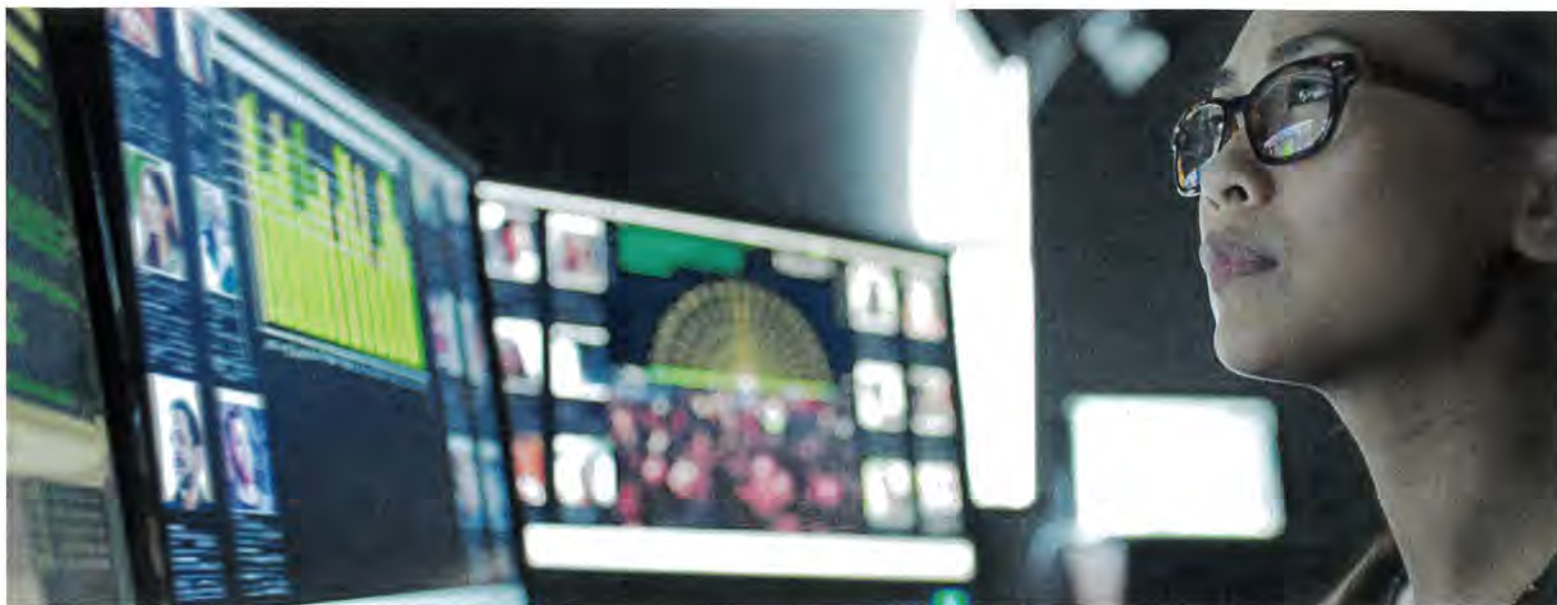
There is considerable variation in the types of facial recognition technology, who uses it, the purposes for which it is used and use settings (e.g., commercial, private security, government and law enforcement). Facial recognition can also be quite technical and cause confusion over terms that may have different meanings in the field versus everyday contexts. Due to the variety of uses, it is difficult to generalize about technology and more difficult still to conceive one-size-fits-all policies; however, the technology is well-established for many uses and rapidly expanding in others due to natural advantages it has over other biometric technologies and increasing affordability, ease of deployment and processing speed.

Government and Law Enforcement Use

Most Americans expect police to use every lawful method at their disposal to protect our communities. For well over a decade, federal, state and local law enforcement have used facial recognition technology as an effective tool in investigations. Many public safety officials feel that this biometrics technology is becoming a game-changer for keeping our communities safe, much like fingerprinting and DNA matching when they came into widespread use, pointing to instances where crimes would have never been solved or prevented without it (examples follow).

Facial recognition has demonstrated value to help narrow searches for suspects more quickly, find missing children, rescue human trafficking victims, exonerate the innocent, identify the deceased and other efforts to assist the public. In these uses, the technology does not make a positive identification but rather makes a first pass at suggesting potential matches. Police routinely do the same thing manually by looking through hundreds of mugshots with victims or canvassing areas with photos. They also routinely search for suspects by name only; criminals use aliases and fraudulent identities every day, harming public safety by slowing time-critical investigations and wasting taxpayer resources. Additionally, searching for a common name (e.g., John Smith) could yield hundreds of results that must be narrowed down using traditional methods. Facial recognition technology simply automates and improves the first step in these processes to identify potential matches.

Questions raised about government use, particularly by law enforcement, have generated the most confusion and concerns regarding facial recognition technology; however, there are many successful law enforcement uses of facial recognition in the U.S. under established policies and procedures that address transparency, use limitation, data security and other privacy-related issues. The [Bureau of Justice Assistance](#) at the U.S. Department of Justice has developed a model policy development template for use by law enforcement, and use cases and related policies across the country have been detailed in the Integrated Justice Information Systems Institute's [Law Enforcement Facial Recognition Use Case Catalog](#).



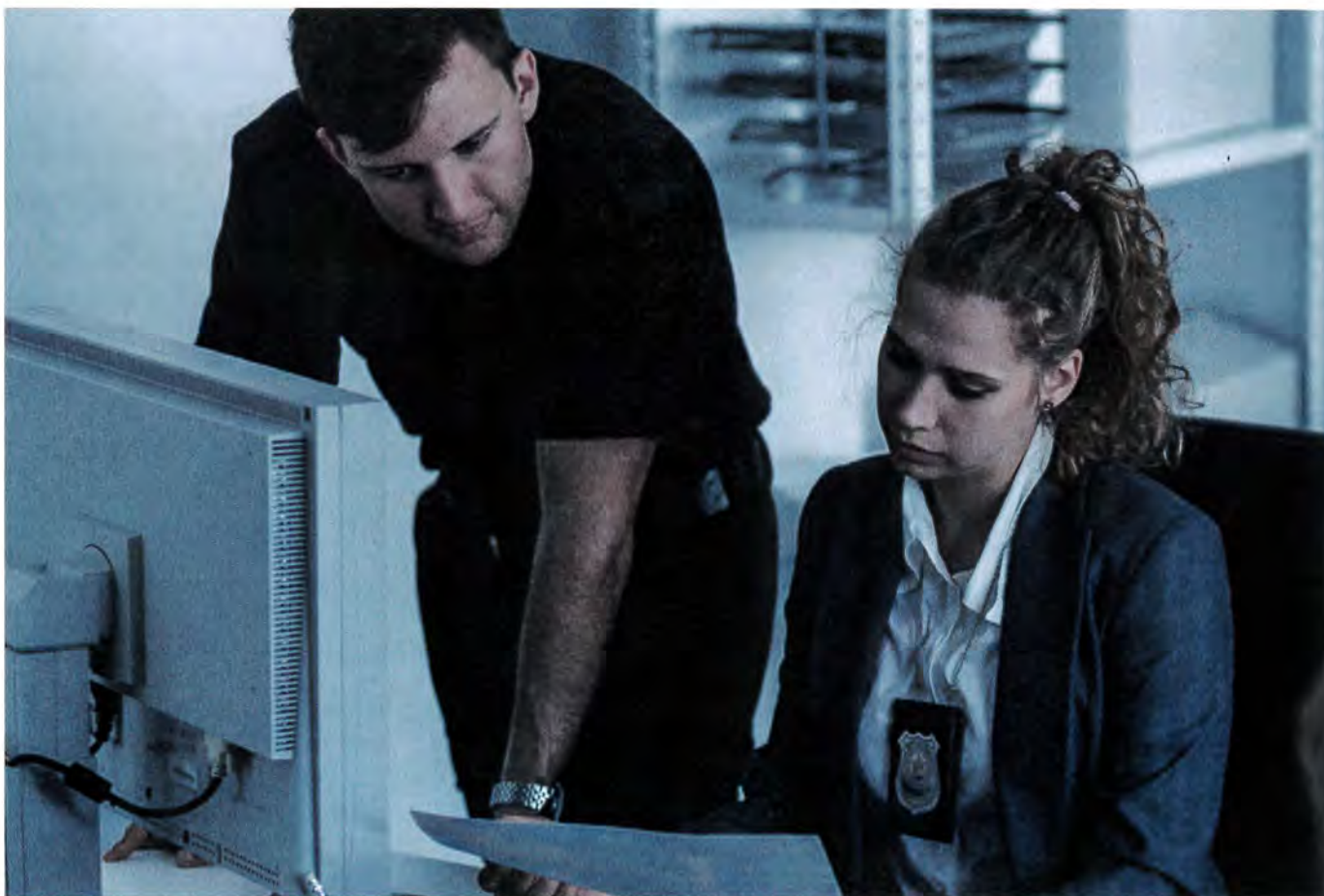
Myths vs. Facts

It is critical that community leaders and the public understand basic facts about facial recognition. Good policy must be fully informed by the facts, not a misleading picture of facial recognition technology and its real-world uses. Below are some common myths along with facts about how facial recognition works and is used in the U.S., many involving police or government use.

MYTH 1: Use of facial recognition technology in the U.S. is “out of control” with no safeguards.

FACTS: Far from a rules-free environment, use of this technology is subject to an existing framework of laws, regulations, administrative rules and best practices that address many privacy and civil liberties concerns. Government use is bounded constitutionally by the First, Fourth, Fifth and Fourteenth Amendments, which prohibit use to suppress free speech and religious expression and protect citizen’s rights to due process and equal protection and against unreasonable searches and seizures. Both public and private entities are subject to the Civil Rights Act and other state and federal anti-discrimination laws.

In another example, federal law clearly allows states to share driver’s license data, including digital photos with federal agencies, but only for law enforcement and other narrow purposes. Many states query their motor vehicle and criminal records databases using the technology to fight fraud and identity theft – uncovering [thousands of fraud cases each year](#) – and assist state and local law enforcement investigations; some states do so if requested by the Federal Bureau of Investigation (FBI), but only subject



to voluntary information-sharing agreements with specific parameters. The [privacy policy](#) for the FBI's program shares in great detail the procedures the agency and its state partners follow in handling and safeguarding data used in facial recognition searches. Sound use policies play a key role in protecting privacy. The [American Association of Motor Vehicle Administrators](#) has also developed a set of facial recognition best practices and model policies that address these concerns. Most biometrics technology providers have recommended use policies and training that guide end users on applications such as data capture, data retention and notifying subjects of biometric collection practices in a transparent manner.

As use of facial recognition for commercial purposes rapidly grows, there are several important data privacy considerations. For commercial, non-security use, SIA supports the [Privacy Best Practice Recommendations](#)

[for Commercial Facial Recognition Use](#) developed by the National Telecommunications & Information Administration through public-private sector collaboration. The best practices cover aspects of deployment including transparency, data management, third party disclosure and security safeguards.

MYTH 2: You can be misidentified by law enforcement due solely to facial recognition errors.

FACTS: Despite provocative reports' concerns about technology errors causing "misidentification" and their implications, **the bottom line is that in investigative applications, facial recognition technology itself does not make a final match determination and therefore cannot identify a person as someone they are not.** A "false positive" is not misidentification; it is part of how the process works to create a gallery of potential matches based on a similarity score. In all known U.S. law enforcement use cases, a facial recognition search is just one part of an identification process requiring a human examiner to confirm whether one of the computer-provided potentially matching photos actually matches the submitted image. There is also a misunderstanding of what accuracy means when it comes to facial recognition technology. Under the National

Institutes of Standards and Technology (NIST) [Facial Recognition Vendor Test Program](#) – known as the gold standard for algorithm testing – accuracy is defined as the likelihood that a matching photo from a database is produced as one of the candidates (in a 1:N search). An "inaccurate" result in the real world simply means that the system fails to retrieve the matching photo, the technology would not be able to assist with identification and other means would be used. If a system is configured to return three photos with the highest scores and the search is successful, one will be a match and two will be false positives. Returning false positive match candidates does not indicate that system is flawed since it is designed to create a gallery of

Trained forensic examiners performed best when supported by facial recognition technology and the most accurate performance resulted when these efforts were combined.

potential matches. Search results are not considered evidence; they can only supply investigative leads that may or may not prove of value. A final determination of whether a match exists is made visually by trained law enforcement analysts. Further steps to verify an individual's identity are part of the police work following this visual determination. Typically, candidate images are deleted after this process, while an auditable record of the query is retained.

MYTH 3: Facial recognition technology has an inherent racial bias that justifies a complete ban on its use.

FACTS: Technology developers strive to make continual accuracy improvements that help systems match successfully and consistently from large sets of photos representing all population segments. In some cases, facial recognition algorithms were tested and found to have more difficulty identifying women and individuals with features common to certain ethnic groups relative to others; however, statistical inconsistency in performance, where found, is not "bias" in its everyday (versus academic) context. More importantly, **the argument that algorithms perform less effectively across the board for African Americans and females isn't factual.**

Recent research suggests that newer algorithms, including many of the [top-performing ones](#) tested by NIST, have accuracy rates for African Americans equal to or even higher than those for other groups. According to NIST, between 2014 and 2018 facial recognition software got 20 times better overall at searching a database to find a matching photograph. After testing 127 software algorithms from 39 different developers – nearly all the leaders in the field – the combined failure rate was just 0.2 percent,

regarding a one-time test of Amazon Web Services' (AWS) Rekognition, a cloud-based tool for "identifying people, objects and scenes." According to the ACLU, it gathered 25,000 publicly available arrest photos and, using the software, ran a search against official photos of the 535 members of Congress, returning "false matches" for 28 of them. The ACLU claimed that since 11 of these matches, or 40 percent, were people of color, and only 20 percent of Congress overall are people of color, there is evidence of racial

bias in facial recognition systems. One of several critical flaws in this analysis is that it used a low accuracy threshold of only 80 percent – casting significant doubt on its methods and conclusion. A lower threshold may be effective enough for other uses such as finding out which president or first lady you might look like, but the ACLU cites these results as justification for a complete ban on law enforcement use of facial recognition. For most public safety purposes, technology providers recommend setting accuracy thresholds

meaning systems were 99.8 percent accurate compared to 96 percent accurate four years before. Consistent performance across all demographic groups is a crucial issue that deserves further study and review and should be a key objective of facial recognition technology developers. Inconsistencies are being mitigated as developers use more diverse data sets and improve facial point collection and algorithms, according to researchers at IBM and the Massachusetts Institute of Technology.

However, calls for banning the technology misunderstand the role of accuracy rates in everyday usage of facial recognition systems and misconstrue the real-world implications when algorithms may not work as well as intended.


Much of the concern about racial bias was fueled by a 2018 American Civil Liberties Union (ACLU) [blog post](#)

as high as possible given current performance levels. AWS later conducted a similar test of the software using a 99-percent threshold and a vastly larger and diverse data set of 850,000 images – which returned zero "false matches" for members of Congress.

MYTH 4: People can match faces better than computers.

FACTS: Facial recognition technology can be as good as or even [better than humans](#) in determining whether two photographed images are of the same person and can do so in a fraction of the time. Human reviewers can also be prejudiced in ways computers cannot. In the [most comprehensive examination to date](#), a team of scientists from NIST and three universities evaluated and compared the performance of people with varying levels of face recognition training against their facial recognition





Responsible use of facial recognition technology means ensuring appropriate transparency and accountability measures, stakeholder education, privacy considerations and civil liberties protections.

algorithm counterparts and found that highly trained forensic examiners performed best when supported by facial recognition technology and the most accurate performance resulted when these efforts were combined.

This means that in addition to automating an otherwise manual process, facial recognition contributes to more accurate identification. 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 U.S. later overturned by DNA evidence. A blanket ban on the technology, which would force investigators to rely heavily on eyewitness identifications, actually puts community residents at greater risk of being “misidentified.”

MYTH 5: Americans are generally fearful of facial recognition technology and want strict limits.

FACTS: There is evidence to suggest most Americans have not accepted provocative claims about the technology. A rush to restrict facial recognition – while popular with some politicians – may not have robust public support. In a [recent national survey](#) of over 3,000 Americans, only 26 percent believed the federal government should strictly limit the use of facial recognition technology, dropping to 18 percent if limits would come at the expense of public safety.

MYTH 6: U.S. government facial recognition systems at airports are illegal and violate privacy rights.

FACTS: During the rollout of biometric entry-exit systems using facial recognition systems at U.S. airports by U.S. Customs and Border Protection (CBP), activists have made numerous false claims. The CBP has [laid out the facts](#) about this program, and many of the misleading claims have been identified and [refuted in detail](#) by the International Biometrics + Identity Association. The legal authority has been provided in numerous acts of Congress and executive actions, and the necessary handling and protection of U.S. citizen data to carry out the program is conducted in a very clear and well-defined process. In addition to the homeland security benefits, deployment of these systems has resulted in decreasing wait times and an improved travel experience. For example, Atlanta gate operators [reported](#) having reduced wait time for boarding international flights to an average of nine minutes.

MYTH 7: If your “faceprint” data is stolen, hackers or others can track you wherever you go.

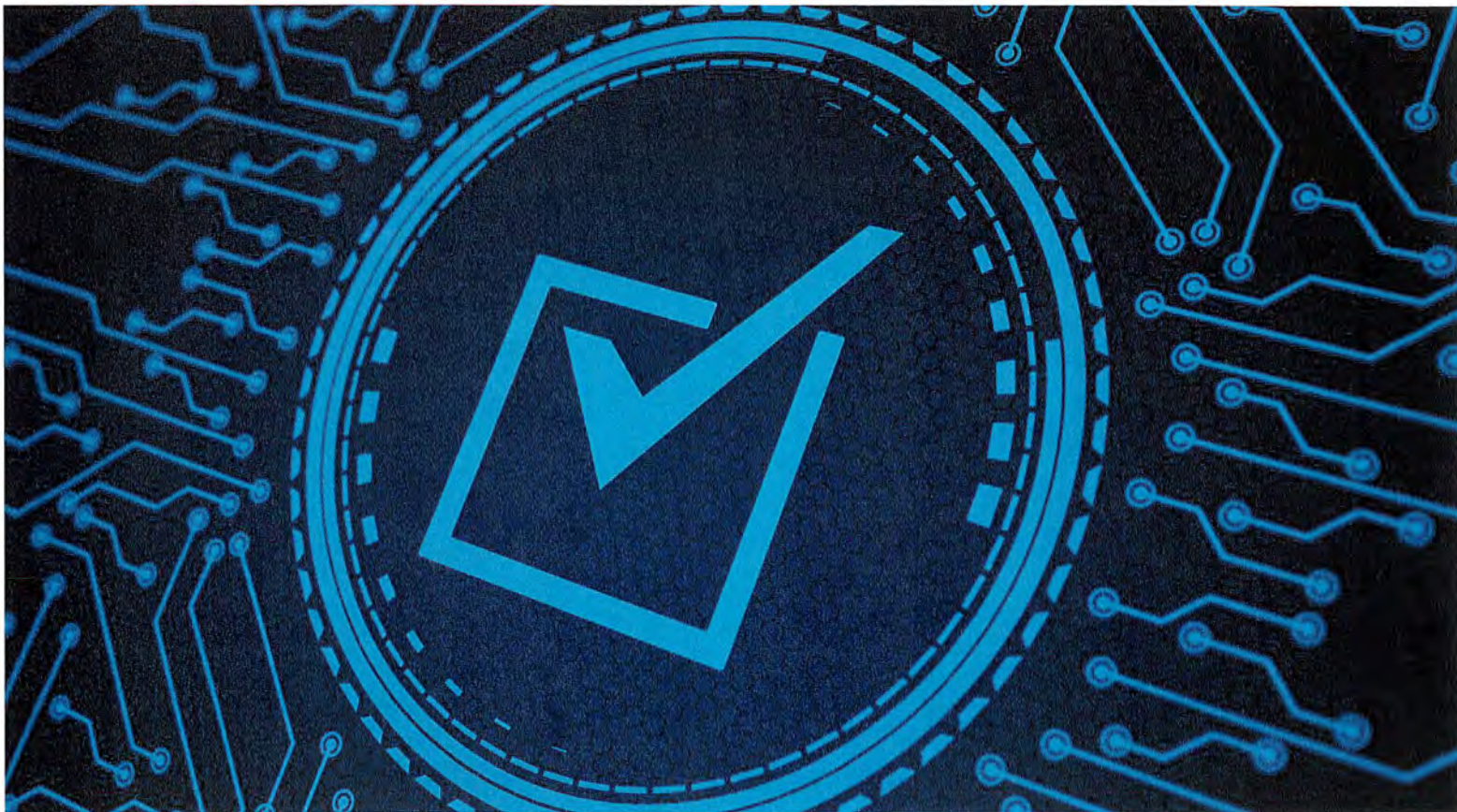
FACTS: During electronic enrollment, a digital photo is translated into a numerical abstraction based on features of the face, creating a unique code or faceprint that is then associated with the identity in the database. The image itself is often not stored, offering greater security and privacy. From a technological standpoint, **if the faceprint is compromised, the process cannot be reverse-engineered to create an image based on the unique code.** It also generally cannot be used in a different system, since all facial recognition system providers use proprietary algorithms, which are not interoperable, to create and read the code, making it even more difficult for the data to be misused.

Reasonable (and Unreasonable) Safeguards

SIA believes any effort to establish additional constructive rules should not unreasonably restrict use of modern technology tools that have become essential to public safety. Responsible use of facial recognition technology means ensuring appropriate transparency and accountability measures, stakeholder education, privacy considerations and civil liberties protections; however, agenda-driven proposals not based on sound information can easily become nonsensical or unworkable. For example, several policy proposals have included impractical or unwarranted use stipulation, like requiring probable cause *before* facial recognition can be used as an investigative tool. The problem is, without knowing the identity of the person sought (the reason to use facial recognition), establishing probable cause is impossible. Other proposals would limit the use of facial recognition

searches only to subjects accused of “serious” crimes and/or to databases of mugshots only – as if some crime victims deserve only limited investigative resources and serious crimes are only committed by those with criminal records. Thus far, most of these proposals have failed at the state level.

Some policymakers and leaders in the tech industry have called for establishing a more consistent legal and regulatory framework that would reassure the public about how facial recognition technology is being used and ensure that accountability measures and use policies are being followed. U.S. tech industry leaders like Amazon and Microsoft have identified principles to guide potential [new rules and legislation](#) and [product use and development](#). Safeguards are much more sensible than prohibitions, and policymakers should start with working towards greater transparency and accountability measures that will generate the data and insight needed for a more informed discussion on what additional policies may be prudent. Representing industry, SIA will continue to engage with other stakeholders in constructive dialogue on these issues.



Examples of Facial Recognition Technology Uses

Below are success stories demonstrating the value facial recognition can provide – the types of successes that would be prevented by arbitrary limits on the technology.

Missing Children

Facial recognition technology has been used around the world to help locate missing children by efficiently searching for and matching images of missing children with photographs of known children. For example, the [National Center for Missing and Exploited Children](#) has used facial recognition technology for years, and in 2018 the city of [New Delhi](#) launched a trial that was able to positively identify 2,930 missing children in just four days.

Border Security

Under the Federal Aviation Administration Reauthorization Act of 2018, the Transportation Security Administration and CBP continue to have joint authority to collaborate on many biometric initiatives, including deploying facial recognition readers in more U.S. airports to check foreign travelers against their identifying travel documents, including passports and visas, to mitigate travel document fraud, a key element of terrorist strategies.

- **Detecting Passport Fraud**

Within the [first three days of deployment](#) at Dulles International Airport, a man trying to use a fake passport was detected that would have easily gone undetected with visual inspection alone. [According to CBP](#), use of the technology prevented 26 alleged imposters from entering the United States in a three-month span in 2018.

- **Faster Airport Processing for All**

The use of facial recognition at airports not only expedites the identification of fraudsters but also improves the speed of processing for all persons who go through security checkpoints. [San Jose International Airport is reducing the length of lines at passport control](#) by using facial recognition systems that can match travelers to documents in less than a second.

- **Effective Facial Recognition at Land**

Borders

Airports are not the only facilities at which people cross borders; those crossing land borders also need to be checked to ensure they are who they say they are. [CBP uses facial recognition at its Port of San Luis border crossing](#) and in February 2019 identified an alleged imposter trying to use a passport that didn't belong to him – the latest of a number of imposters detected since the project began in late October.

- **Secure and Rapid Sea Border Processing**

CBP has the same need to ensure security on cruise ships. Because of the number of people who board and exit cruise ships, it is crucial that any security system allow for rapid verification of identity. [Royal Caribbean Cruise Lines is implementing a facial recognition system](#) that will provide the same secure and rapid border processing being deployed in some airports and is receiving “very positive guest feedback” from this initiative.

Confirming True Identity

Of course, border security systems are of limited value if documents themselves are authentic but fraudulently obtained. In conjunction with the federal government, states are improving their secure document issuance systems to ensure that people are who they say they are. These improvements allowed the [Arizona Department of Transportation](#) to identify a person with multiple stolen identities. Similarly, the [Iowa Department of Transportation](#) identified a North Carolina prison escapee through facial recognition. A few years ago, New Jersey officials reported they had identified 69 people attempting to fraudulently obtain driver's licenses; [New York has identified 4,000 fraudsters](#).

Law Enforcement

Law enforcement officials have benefited immensely from leveraging facial recognition technologies; here are a few examples of successes.

- **Annapolis Capital Gazette Shooting**

In June 2018, a gunman entered the Annapolis Capital Gazette building and shot and killed five employees. Police sent an image of the attacker to the Maryland Combined Analysis Center, which helped [identify him](#) by comparing the photo to others in the Maryland Image Repository System.



- **Sexual Assault Cold Cases**

In 2017, the FBI deployed facial recognition technology to identify and apprehend a fugitive accused of sexually assaulting a minor after matching a photo of the suspect with an acquired U.S. passport. The man was apprehended in Oregon after a 16-year manhunt. Similarly, in 2014, the FBI used facial recognition technology to help locate and apprehend a [convicted pedophile](#) who had been on the run for 14 years.

- **International Law Enforcement**

Facial recognition is also used for cross-border criminal identification. [Interpol's facial recognition service](#) was used to identify someone wanted for murder in the Czech Republic. He had evaded arrest for ten years until authorities in Argentina conducted a search using the service, identified him and made an arrest within 48 hours.

Fraudulent Activity

Often, criminals acquire and present fraudulent identification documents to subsequently obtain access or services, such as unauthorized entry into sensitive areas, credit card and other debt obligations under other individuals' identities, and fraudulent access to Medicaid and welfare benefits. Facial recognition technology can be used to help identify individuals committing these types of fraud.

- **Stolen Credit Card Mitigation**

According to the [Arapahoe County Sheriff's Department](#), an unknown woman pictured in

surveillance photos entered a Colorado store and attempted to purchase items with a credit card stolen from a vehicle earlier that day. The transactions could not be completed, as the cardholder had already canceled the stolen cards. Checking the surveillance photos against a correctional mug shot database with the agency's facial recognition application revealed the identity of a high-probability candidate who is now under investigation for use of the stolen credit card.

Storefront Security

Organized retail crime in the U.S., such as shoplifting and cargo theft, continues to rise. According to a 2018 survey by the [National Retail Federation](#), three out of four retailers report they have seen an increase in such crimes in the past year. Retailers who have integrated facial recognition technology have seen benefits in deterring these crimes.

Mobile Banking

Apple cultivated a new era of mobile biometric authentication by replacing the Touch ID login feature with Face ID, which allows consumers to access their iPhones using their unique facial features. The seamless interaction between consumer and mobile device now enables the financial sector to channel the iPhone's Face ID and conduct mobile banking transactions while instituting Apple's biometric authentication feature.



securityindustry.org