



June 3, 2019

The Honorable Elijah E. Cummings
Chairman
House Committee on Oversight and Reform
2157 Rayburn House Office Building
Washington, DC 20515

The Honorable Jim Jordan
Ranking Member
House Committee on Oversight and Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Cummings and Ranking Member Jordan:

On behalf of the Security Industry Association (SIA), thank you for holding a series of important hearings on facial recognition technology. SIA represents nearly 1,000 companies that provide safety and security technology solutions vital to public safety, protecting lives, property, information and critical infrastructure.

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. However, arbitrary limits will harm Americans who benefit from it in countless but underpublicized ways, improving privacy and security through more accurate identity authentication and other benefits for consumers and society.

We are concerned that recent calls to completely ban the use of facial recognition technology at various levels of government are based largely on a misleading picture of how the technology works and its real-world uses in the United States. Such calls 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. I encourage you and your staff to review the attached SIA publication, which explains seven myths and related facts regarding government use of facial recognition.

Responsible use of facial recognition technology that ensures appropriate transparency and accountability measures, stakeholder education, privacy considerations and civil liberties protections. Further actions may be needed to reassure the public about how facial recognition technology is being used and ensure that proper policies are being followed. However, such actions must be based on sound information and analysis and involve input from stakeholders with expertise on the technology.

SIA and our members stand ready to contribute to constructive dialogue surrounding facial recognition technology. Please let us know if there is any way we can assist you as you continue to examine these issues.

Sincerely,

A handwritten signature in black ink that reads "Don Erickson". The signature is written in a cursive, flowing style.

Don Erickson
CEO
Security Industry Association

Face Facts: Dispelling Common

MYTHS

Associated With Facial
Recognition Technology



securityindustry.org

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

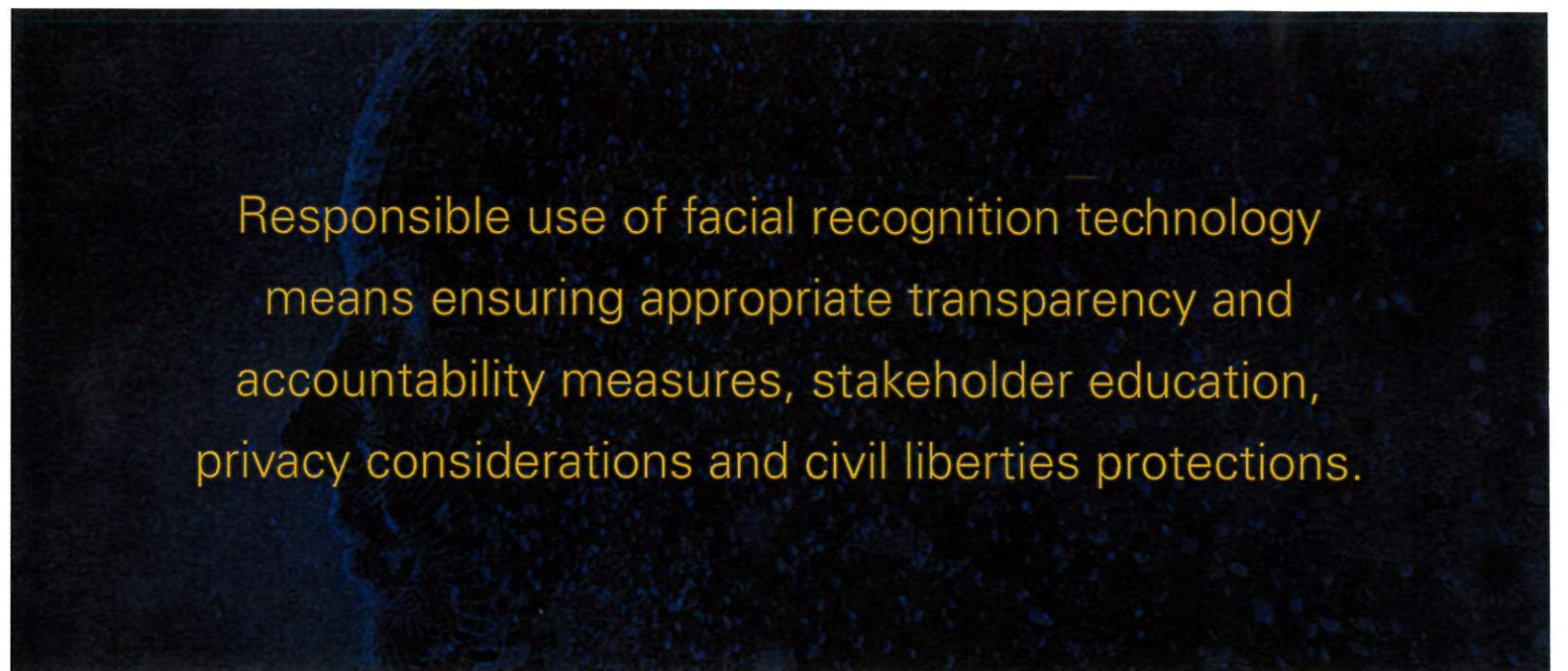
Of course, border security systems are of limited value if documents themselves are authentic but fraudulently obtained. In conjunction with the federal government, states are improving their secure document issuance systems to ensure that people are who they say they are. These improvements allowed 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.



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.

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.**

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](#).

