Statement of Jake Parker
Senior Director of Government Relations
Security Industry Association

Before the

House Committee on Oversight and Reform

United States House of Representatives

"Facial Recognition Technology (Part III): Ensuring Commercial Transparency & Accuracy"

January 15, 2020

2154 Rayburn House Office Building

Good morning Chairwoman Maloney, Ranking Member Jordan and distinguished members of the Committee. My name is Jake Parker, Senior Director of Government Relations for the Security Industry Association (SIA). SIA is a nonprofit trade association representing more than 1,000 businesses that provide a broad range of security products and services in the U.S. across government, commercial and residential sectors – and employ thousands of technology leaders.

Our members include many leading developers of facial recognition technology, among them nearly 20 companies participating in the NIST evaluation program, and many others that offer products that incorporate or integrate with this technology for a wide variety of security and public safety applications. These range from technology start-ups and small businesses to large corporations.

I appreciate the opportunity to provide collective input from our industry on this important matter of ensuring our technologies are used consistently with our values. Above all, we believe all technology products, including facial recognition technology, must only be used for purposes that are lawful, ethical and non-discriminatory. Specifically, we believe facial recognition makes our country safer and brings value to our everyday lives when used effectively and responsibly.

Use of Facial Recognition Technology Offers Tremendous Benefits

In the private sector, facial recognition has offered tremendous benefits, primarily through allowing individuals to securely, quickly and conveniently prove their identity to enter a venue, board a plane, perform online transactions and seamlessly access personalized experiences. In addition, facial recognition has enabled private entities to secure their property against individuals seeking to commit violence, theft or other harm.

For example, facial recognition technology is able to 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. Biometric entry systems, such as those developed by our members, can provide additional convenience for registered users. In another example, the technology is being used to reduce organized retail crime (ORC) and theft, which has skyrocketed in recent years, hurting American businesses, consumers and taxpayers alike.

Government agencies have made effective use of facial recognition technology for over a decade to improve homeland security, public safety and criminal investigations. A notable success story is the use of the technology to identify and rescue trafficking victims. One such tool has reportedly been utilized in almost 40,000 cases in North America, identifying 9,000 children and over 10,000 traffickers. According to a Wired article last year, a law enforcement officer in California ran across a Facebook post from the National Center for Missing and Exploited Children with a picture of a missing child. The child, who had been victimized for weeks, was successfully recovered after law enforcement ran the photo through this system and conducted an investigation based on the leads it generated.

These benefits across both public and private sectors have been driven by technological advances that enhance the natural advantages facial recognition provides over other biometrics. This includes the massive, well-documented improvements in accuracy over the past 3-5 years and shrinking costs that have increased interest from customers and competition among suppliers.

Sound Policy, Oversight and Guidance

We believe transparency should be the foundation that governs the use of facial recognition technology, for both commercial and government use. It should be clear when and under what circumstances the technology is used as well as the processes and procedures governing the collection, processing, storage, use and transfer of related data. Our industry supports sensible safeguards that promote transparency and accountability measures as the most effective way to ensure responsible use of the technology without unreasonably restricting tools that have become essential to public safety. SIA does not support moratoriums or blanket bans on the use facial recognition technology.

We understand the Committee is working proposals that would require greater accountability for federal government use of facial recognition technology. Having greater accountability measures in place would help reassure the public that facial recognition technology is being used effectively and responsibly, by ensuring that established policies are being followed. We look forward to continuing to work with you on these proposals.

The federal government is already playing a positive role in supporting increased accuracy of the technology through the testing and benchmarking activities of agencies like NIST. Congress should provide NIST with the resources it needs to support expansion of these efforts, such as the *Demographic Effects* report released in December, which ultimately supports fielding effective technology through informed vendor selection. Additionally, we urge NIST to consider the possibility of developing a curated and privacy-protected dataset that could be provided to well-vetted developers to help them specifically address the issue of reducing demographic effects in facial recognition technology, given some of significant limitations of the data sets currently used.

Regulation specific to commercial use of facial recognition technology only makes sense in the context of a national data privacy policy that includes biometric information – the subject of a broader ongoing debate. In the meantime, industry can play a more active role in providing users with the tools they need to implement robust policies for responsible use. SIA and our members are working to do just that by developing a set of use principles for facial recognition technology.

Implications of the NIST *Demographic Effects* Report

Industry supports and appreciates NIST's work as we strive to provide world class technology to our customers. It's important to note that participants have been working closely with NIST for decades, handing over their technology and allowing the government to serve as a 3rd party evaluator, which entails granting NIST permission to rigorously test and publicly post the results. In recent years the evaluation has shown facial recognition technology is in a continual cycle of improvement.

The most significant takeaway from the NIST report is that it confirms current facial recognition technology performs far better across racial groups than is widely reported. In contrast, according to NIST's data, only 4 out of 116 algorithms tested using the Mugshot Identification Database had false match rates more than 1% for any demographic, male, female, black, white, Asian or American Indian.

One of the algorithms cited by NIST as an example demonstrated a 0.025 % false match rate for black males and 0.1% for black women. While in relative terms this is 10 times higher for black women (compared to white males) and 2.5 times higher for black males, these error rates are all at or below one tenth of one percent.

NIST has documented that the facial recognition software it tested is now over 20 times better than it was in 2014 at searching a database to find a matching photograph. Of note, NIST's September 2019 report found "close to perfect" performance by high-performing algorithms with miss rates averaging 0.1%. On this measurement, the accuracy of facial recognition is reaching that of automated fingerprint comparison, which is generally viewed as the gold standard for identification. Given these strong results, our members feel comfortable deploying facial recognition technology with appropriate transparency and privacy safeguards.

Most importantly, the report provides a critical benchmark against which developers can work improve the technology. The results are a snapshot – NIST will be able to track industry progress over time through the ongoing evaluation program. We have already seen major improvements and I am confident this will continue.

Context Within Operational Systems

While our members are not currently seeing instances of demographic differences in widely used algorithms affecting the performance of facial recognition systems in high risk settings, developers and end-users have a responsibility to minimize any negative effects that could result from technology errors, though proper design, configuration, policies and procedures.

Many facial recognition implementations involve human review as an integral part of the process – whether to verify someone's identity for a banking transaction, or to investigate someone further due to a potential crime. No decisions are made solely on the score matches of the algorithm in these cases. In a 2018 study, NIST found that facial recognition was most accurate when technology was combined with trained human review.

In one example from August last year, as reported by the New York Post, NYPD detectives used the technology to identify a man who sparked terror by leaving a pair of rice cookers in the Fulton Street subway station. Within minutes, detectives pulled still images of a suspect from security footage and used facial recognition software to compare them to mug shots in the NYPD's arrest database. The system returned several hundred potential matches, and after multiple stages of human review, it took NYPD only one hour to identify the suspect.

According to the head of the NYPD facial recognition unit, Sgt. Edwin Coello, "Five years ago you probably have endless detectives looking through videos and images of arrested individuals based on descriptions…It could take several hours or several days. This is the most important type of case that we'd see out there: a possible terrorist attack in NYC."

In addition to automating an otherwise manual process, facial recognition contributes to more accurate identification. Without the technology, we are left with far less effective and less accurate manual processes – with potentially serious safety and security consequences.

Conclusion

On behalf of SIA, I appreciate the opportunity to provide collective input from our industry on this important matter. I will do my best to answer any questions you may have, however if there is any information requested that I cannot provide today, I will be happy to work with our members to provide helpful information.