Security Industry Association
Silver Spring, Maryland

Testimony Before the Finance Committee
Maryland Senate

Opposition to Senate Bill 476

Drake Jamali
SIA Manager of Government Relations
March 11, 2020
Annapolis, Maryland

Chairwoman Kelley, Vice Chairman Jennings and members of the Committee, thank you for this opportunity to speak with you today. The Security Industry Association (SIA) is a nonprofit trade association representing businesses that provide a broad range of security products for government, commercial and residential users, including over 20 businesses with headquarters, employees and operations in Maryland.

Our members include many of the leading developers of facial recognition technology as well as those incorporating this technology into a wide variety of security and public safety applications. I appreciate the opportunity to provide input from industry on the important matter of ensuring our technologies are used consistently with our values. SIA believes 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.

The tremendous benefits of this technology are well-established in both public and private sector applications. Government agencies across the nation have made effective use of it for more than a decade to improve homeland security, public safety and criminal investigations. For example, it has been used with great success to rescue human trafficking victims, identifying 9,000 missing children and over 10,000 traffickers. In one case last year, a law enforcement officer in California saw a social media post about a missing child from the National Center for Missing and Exploited Children. After law enforcement used facial recognition technology the victimized child was located and recovered. In another example last year, NYPD detectives used the technology to identify a man who sparked terror by leaving a pair of rice cookers in a subway station. Using facial recognition technology, along with human

review, detectives were able to identify the suspect within an hour. The Chief of Detectives was quoted saying, “To not use technology like this would be negligent.”

The bill under consideration today would immediately take these critical tools off the table for law enforcement throughout the state – putting the safety of every resident at risk despite the lack of evidence that significant unlawful use or misuse of the technology is occurring. And while most concerns expressed about the technology have centered on law enforcement, it is clear the bill would go far beyond this to ban other established uses like secured employee access to buildings, systems that protect occupants at government facilities and software that detects fraud against government programs, to name a few. In fact, because the problematic definition used for the technology is so broad, the ban on “face surveillance” would prohibit any government official, employee, contractor, or vendor from using any technology with facial recognition capabilities, including social media sites and smartphones, regardless of whether it has anything to do with surveillance.

Before taking the extreme step of banning all possible government applications of the technology, now and in the future, we urge policymakers to thoroughly examine how the technology is used and address the issues at hand after fully considering the options available. For example, we believe sensible transparency and accountability measures can be identified that would ensure responsible use of the technology without unreasonably restricting tools that have become so essential to public safety.

Unfortunately, the justifications typically cited for banning facial recognition technology are based on several misconceptions, often taking accuracy rates and related scientific terminology out of context. “False positive rates” should not be confused with misidentification. Many facial recognition implementations involve human review as an integral part of a process. The technology is used as a first step in photo comparison that would otherwise be done visually – but there is no automated decision-making. All known law enforcement applications in the U.S. require a trained investigator to confirm whether any computer-suggested photos from a database matches the person in a submitted image, typically after it has returned a set number of photos with the highest similarity scores for every search.

While there will always be always be error rates for any biometric, consistent performance across all demographic groups is a critical goal for developers to address oft-cited

concerns about facial recognition "bias." The National Institute of Standards and Technology (NIST) recently evaluated many leading algorithms across race and other demographics, finding that current technology performs far better across racial groups than had been widely reported. We believe there will be continual improvements, and context is important as NIST also documented last year that the software is over 20 times better than it was in 2014 at searching a database to find a matching photo. Its 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. To be sure, without this technology we are left with far slower and less accurate processes – with potentially serious safety and security consequences.

For all of these reasons, we urge you not to advance this bill in its current form and suggest that further examination and multi-stakeholder dialogue on these issues should be undertaken before resorting to such a wide-ranging ban on a technology that is becoming so critical to public safety.