FACE FACTS: HOW FACIAL RECOGNITION MAKES US SAFER & THE DANGERS OF A BLANKET BAN

Facial recognition technology makes our country safer and brings value to our everyday lives when used effectively and responsibly. The Security Industry Association (SIA) believes all technology products, including facial recognition technology, must only be used for purposes that are lawful, ethical and nondiscriminatory.

- **Modern facial recognition technology is highly accurate.** The National Institute of Standards and Technology (NIST) found that the facial recognition software it tests is now over 20 times better than it was in 2014 at searching a database to find a matching photograph. NIST's September 2019 report found "close to perfect" performance by high-performing algorithms with miss rates averaging 0.1%, reaching the accuracy of fingerprint comparison technology – the gold standard for identification.

- **The benefits of facial recognition have been proven for more than a decade** of use in real-world applications, including finding missing and exploited children, protecting critical infrastructure and aiding law enforcement investigations. See examples of the benefits in action on the reverse page.

WHY A BLANKET BAN PUTS AMERICANS AT RISK

- **A blanket ban on government use precludes all possible current and future applications of the technology,** regardless of the purpose, putting the safety of every resident at risk. Beyond law enforcement, such **a ban prohibits other proven uses** like secured employee access to critical infrastructure and other systems that protect building occupants and software that detects fraud against government programs, to name a few. **Such bans have also been defined broadly**, prohibiting any government official, employee, contractor or vendor from using any technology with facial recognition capabilities, including social media platforms and smartphones.

- **A ban on facial recognition eliminates a useful tool that is being used alongside human intelligence.** Thorough analysis must acknowledge the alternatives a ban would leave us with – far slower and less accurate identification processes that are much more prone to errors (for example, detectives sifting manually through hundreds or even thousands of videos and images of arrested individuals based on suspect descriptions). NIST confirmed in a 2018 study that the highest identification accuracy is achieved through human analysis supported by facial recognition technology versus either element alone. That's why it has been used in thousands of investigations without a single example of an innocent person being falsely arrested due to a misidentification.

- **Before taking such an extreme step,** policymakers must thoroughly examine how the technology is used and consider all the options available to address concerns. 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.

- **Bans threaten U.S. competitiveness in the tech space** by ceding the market and shifting the world's security infrastructure to other countries investing in the technology like China and Russia.

FACE FACTS: REAL STORIES OF FACIAL RECOGNITION KEEPING AMERICANS SAFE

SAVING SEX TRAFFICKING VICTIMS – In April 2019, a California law enforcement officer saw a social media post about a missing child from the National Center for Missing and Exploited Children. The officer used facial recognition which returned a list of online sex ads featuring the girl. According to a story in WIRED, the girl had been "sold for weeks," and the officer's actions helped a process that "recovered and removed from the girl from trauma."

CATCHING A NEW YORK CITY SUBWAY TERRORIST – In August 2019, New York Police Department detectives used facial recognition to help identify a man who sparked terror by leaving rice cookers in and around a subway station. Detectives pulled still images from security footage and used facial recognition software, along with additional investigative work, to identify the suspect within an hour. NYPD officials were quoted saying, "To not use technology like this would be negligent" and "This is the most important type of case that we'd see out there: a possible terrorist attack in NYC."

FINDING A KILLER WHO TARGETED LGBTQ VICTIMS – On May 25, 2019, in Wayne County, Michigan, three members of the LGBTQ community were shot and killed by a man at a local home. The Detroit Police Department used facial recognition, as well as their own intelligence, to help identify the suspect based on video from a nearby gas station.

IDENTIFYING THE CAPITAL GAZETTE KILLER – Jarrod Ramos was angered by a story the Capital Gazette Newspaper in Annapolis, Maryland, ran about him in 2011 and brought a lawsuit against the paper for defamation, which a judge later dismissed. In June 2018, Ramos entered the newspaper building with a shotgun and killed five employees, leaving two others critically injured. Anne Arundel Police obtained an image of Ramos and sent it to the Maryland Combined Analysis Center, which helped identify him by comparing the photo to others in the Maryland Image Repository System.

APPREHENDING PEDOPHILES EVADING JUSTICE – In 2017, after a 16-year manhunt, a man accused of sexually assaulting a minor was apprehended in Oregon. Using facial recognition technology, the Federal Bureau of Investigation (FBI) was able to identify the suspect after a positive match was found when the suspect sought to acquire a U.S. passport. 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.

PREVENTING ENTRY INTO THE U.S. UNDER FALSE IDENTITIES – After just three days of operation, facial recognition technology at Dulles International Airport in Virginia caught a man trying to use a fake passport to enter the United States. The fraudulent passport would have easily gone undetected with visual inspection alone. The ability to enter under a false identity is essential to organized crime, human trafficking, money laundering, drug smuggling, terrorism and many other criminal activities. According to U.S. Customs & Border Protection, use of the technology prevented 26 alleged imposters from entering the U.S. in just a three-month span in 2018.