February 16, 2022

The Honorable Chuck Schumer
Majority Leader
U.S. Senate
Washington, D.C. 20510

The Honorable Mitch McConnell
Minority Leader
U.S. Senate
Washington, D.C. 20510

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives
Washington, D.C. 20515

Dear Majority Leader Schumer, Speaker Pelosi, Minority Leader McConnell, and Minority Leader McCarthy:

On behalf of the Security Industry Association (SIA), which represents over 1,200 companies that manufacture and integrate physical and cyber security solutions vital to the security of the United States, we write regarding the ongoing activity surrounding the federal government's use of facial recognition technology. SIA believes all technology products, including facial recognition, must only be used for purposes that are clearly defined, lawful, ethical, and non-discriminatory. When used appropriately, facial recognition has many proven benefits, such as aiding efforts to reunite victims of human trafficking with their loved ones, executing counterterrorism missions in critical situations, cracking cold cases, facilitating safe travel, and detecting travelers using fraudulent documents to enter the United States.

Following recent events, SIA and its members are committed to partnering with Congress and federal agencies to strengthen public trust on the use of facial recognition technologies. We recognize that the concerns cited by Congress deserve careful consideration, and SIA stands ready to help address each concern with appropriate solutions. However, instead of focusing on legislation that constructs a responsible framework for how facial recognition can be used responsibly and transparently, some critics have continued calls for blanket bans or moratoriums on the use of this technology – both agency specific and across the federal government. SIA opposes this approach, which not only eliminates beneficial applications, but also would degrade U.S. and allied leadership in developing biometric technologies.

SIA requests that Congress consider three recommendations to support improvements in facial recognition policymaking while promoting its transparent use and America's leadership role.

Leverage Relevant SIA Policy Principles to Build Public Trust

To strengthen public trust, SIA published a set of policy principles to serve as a guide to law enforcement, public sector, and private sector entities considering the adoption and deployment of facial recognition solutions.[1] We believe these principles should apply to the implementation of facial recognition tools

[1] See "SIA Policy Principles for the Responsible and Effective Use of Facial Recognition Technology" https://www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

across security and non-public safety applications in both public- and private-sector settings, and should be reflected in development of any organizational or public policies addressing these uses of the technology. Prior to implementation, federal agencies should incorporate the following core principles to build public trust with Congress and U.S. citizens:

- Transparency. Transparency is critical to security and privacy, as it helps build and maintain public trust. It should be clear when and for what purpose facial recognition technology is used as well as which processes and procedures govern the collection, processing, storage, use and transfer of related data. Importantly, transparency should ensure that every application of the technology is subject to a policy set by the implementing organization, which governs how the technology is to be used.
- Clear and Defined Purposes. Organizations using facial recognition must specifically identify their purposes for using the technology; they must understand the capabilities and limitations of the systems they intend to use and ensure that the technology is selected and configured appropriately for that purpose. Similarity thresholds and other performance settings should be highly tailored according to the intended use.
- Using Accurate Technology. Organizations must strive to use the highest-performing facial recognition technology for a given application, with accuracy validated using sound methods, such as through the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) program, the global gold standard for scientific, independent evaluations of facial recognition algorithm performance. Both developers and end users have a responsibility to develop technology using lawfully obtained data and minimize any negative effects that could result from variability in technology performance through proper design, selection, and configuration of the technology, as well as policies and procedures addressing human elements of the application. For example, organizations must have a top performing algorithm validated by NIST that is proven to have a diverse dataset of all ethnicities to ensure there is no racial bias in the algorithm. Additionally, providers have a responsibility to provide training – and retraining, as appropriate – for technology buyers to ensure that such systems are used in appropriate ways.

Furthermore, it is especially important for federal agencies deploying facial recognition for non-public safety applications to delineate if their personnel plan to use facial recognition for identification (1:N comparison) or verification (1:1 comparison) purposes. It is imperative for agency end users to underscore that facial recognition used for verification and identification should not be construed as "mass surveillance." To assuage such concerns, policymakers should include clauses within agency use policies that guarantee constitutional rights and ensure facial recognition technologies do not violate constitutional protections.

Consider Governance Frameworks that Address Biometric Data Collection

Transparency and use policy measures need to be reinforced by comprehensive governance frameworks that stipulate how citizen biometric data is collected, retained, and ultimately scrubbed after a designated period. Specific provisions will vary based on an agency's jurisdiction, intended use case, and standard operating procedures for data collection. Regardless of the aforementioned variables, agencies should follow the models published by the U.S. Customs and Border Protection (CBP) and Transportation Security Administration (TSA) for air travelers opting into the use of biometric technologies for identification and verification.[2] For example, under the privacy section of CBP's biometrics website, it

[2]See CBP & TSA biometrics websites: https://biometrics.cbp.gov/ and https://www.tsa.gov/biometrics-technology

clearly states that "CBP retains U.S. citizen photos for no more than 12 hours after identity verification;" and similarly, TSA's biometrics website states, "TSA retains personally identifiable information (PII) only for as long as is necessary to fulfill the specified purpose(s) of biometric technology pilots…TSA's Privacy Impact Assessments provide guidance on matters such as transparency, specific use limitations, data minimization, and purpose specification for our biometric identity verification pilot."[3] This level of transparency and partnership with industry is part of why aviation deployments of biometric technologies have been so successful and widely adopted, and we strongly encourage agencies to follow CBP and TSA's model prior to deployment.

Another key element that merits consideration is justification for algorithm selection prior to deploying facial recognition solutions. End users should consider and communicate on the performance benchmarks of the selected algorithm, where it ranks on recent and relevant NIST FRVT reports, and note any demonstrable improvements from past years. In 2019, NIST found that top-performing algorithms were both extremely accurate overall and exhibited "undetectable" differences in false positive error rates across demographic groups.[4] Since then, facial recognition technology has continued improving significantly at a transformative pace, and this assertion is validated by the most recent NIST report from January 2022 – where the top 25 algorithms were able to retrieve matching photos at the highest ranked score from a database of over 12 million mugshot images with "miss rates" approaching 0.1%.[5] However, the trust that these significant accuracy improvements helps build can be undermined easily if agencies fail to disclose its biometric data privacy practices and justification for selecting its algorithm/solution.

<u>For Non-public Safety Applications, Emphasize Opt-in and Opt-out Procedures</u>

Non-public safety biometric applications, such as identity proofing, access control, fraud detection, and identity verification, provide critically important functions that help facilitate airport traveler screening, create another layer of authentication to counter identity theft, and reveal when fraudulent documents are in use.[6] User consent should be the cornerstone of implementation framework. While these positive examples serve an important purpose, federal agencies should not require U.S. citizens to submit biometric data by compulsory means. Alternatively, agencies should consider opt-in and opt-out processes to provide citizens with the ultimate say in deciding whether to enroll their biometric data in order to add an additional layer of protection. CBP, for example, allows U.S. travelers use biometric screening services– e.g., GlobalEntry – but if air passengers are uncomfortable submitting biometric data, travelers can voluntarily choose to have their credentials checked by traditional means.

---

[3] CBP and TSA both publish Privacy Impact Assessments: a decision tool to identify and mitigate privacy risks that notifies the public what PII DHS is collecting, why the PII is being collected and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

[4] See *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280, 8,* https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf, and see *What NIST Data Shows About Facial Recognition and Demographics* https://www.securityindustry.org/2020/02/14/what-nist-data-shows-about-facial-recognition-and-demographics/;

[5] See *What Science Really Says About Facial Recognition Accuracy and Bias Concerns,* https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/

[6] For this letter's context, "non-public safety" applications do not pertain to biometric technologies used for investigatory, counterterrorism, or national security purposes.

SIA is committed to work with the committees of jurisdiction to craft legislation that strengthens public trust in facial recognition technologies and ensures their responsible use by government end-users. SIA encourages Congress to work with the private sector to establish clear guidelines and regulations for facial recognition technology in order to strengthen public trust. Thank you for considering SIA's views and recommendations on this important issue.

Sincerely,

Don Erickson, CEO
Security Industry Association