Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

**DISCLAIMER:** Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
January 15, 2022

Office of Science and Technology Policy
The White House
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Sent via email: BiometricRFI@ostp.eop.gov

RE: RFI Response: Biometric Technologies

Airlines for America (A4A), on behalf of its members,¹ offers the following response to the Office of Science and Technology Policy’s (OSTP) request for information, “Public and Private Sector Uses of Biometric Technologies” (Biometrics RFI).² Identity verification is a cornerstone of security and facilitation in aviation. Our members have invested in their own initiatives and worked closely with our partners in the Department of Homeland Security (DHS) to leverage biometric technologies to this end. Our principal goals are enhancing security and improving the passenger experience through the use of biometric identity verification. To accomplish these goals, aviation’s use of biometrics must be fast, accurate and reliable.

Technological advances in recent years have significantly improved facial recognition matching rates across all demographics, and successfully adapted to new passenger environments and requirements, including the mask requirements for COVID-19. We strive for the highest standards in privacy, transparency, consent and security to encourage passenger acceptance and to achieve operational benefits of biometric technology. There are distinct yet complimentary roles that industry and DHS perform in this space, and continued collaboration is critical to meet our goals.

Biometric Verification in Aviation

The use of biometric technology in aviation helps automate identity and citizenship verification requirements with a higher degree of confidence. Airlines verify a passenger’s identity at several points during the customer journey, including check-in, bag drop, lounge access and boarding. The Transportation Security Administration and U.S. Customs and Border Protection also verify a passenger’s identity as part of their security and admissibility processes. In most

cases, these processes are conducted manually, requiring a passenger to present a physical document proving the passenger’s identity, citizenship status and proper entry requirements (e.g., passport, driver’s license, and visa) which is then visually matched to the individual. The benefits of automation are still limited by a need for a traveler to present identity and travel documents and access to appropriate and sometimes multiple government databases. A biometrically enabled travel experience can provide the traveler the choice to opt-in or opt-out of certain facilitation benefits, and at the same time, provide fidelity on how, when, and for what purpose their data is being used.

In Partnership with DHS

In some cases, airlines may partner with DHS in identity verification (e.g., Biometric Exit). An airline may own and/or operate the technology to capture a passenger’s image, then transmits an encrypted image to government secure infrastructure and matching mechanisms to verify a passenger’s identity.

Transforming the Passenger Experience

Some airlines are exploring options to conduct facial matching of the passenger physically present against the airline’s own database of stored images to transform the passenger journey. Biometric verification of passengers creates a true seamless experience for the passenger. This transformation leverages biometric facial matching from check-in to bag drop to boarding, with explicit consent from the passenger. When facial matching is applied throughout the passenger journey, operational efficiencies and security benefits are realized in tandem.

Benefits of Biometric Verification

Biometric verification creates a safer, seamless, and contactless passenger experience, and its convenience and scalability will help airlines adapt to passenger volume growth and operate more efficiently. As the department responsible for the security of air travel, DHS equally benefits from biometric technologies.

Operational Efficiency and Adaptability

Over the past decade, advancements in biometric technologies have demonstrated both security and facilitation benefits. Further, technology has advanced to the point where security and facilitation can be mutually reinforcing. Prior to the COVID-19 pandemic, the growth in domestic and international travel demanded adoption of technology solutions that maximized existing personnel and resources. In the summer of 2018, the World Travel and Tourism Council noted that “the travel industry could create 100 million new jobs in the next 10 years if…supported by infrastructure investments and biometrics and other technologies are deployed to make travelling more efficient and safe.”

---

airline industry will face the same dilemmas it faced in 2019—increasing levels of passenger traffic with limited infrastructure capabilities.

Automating facial matching facilitates the secure and seamless processing of a growing number of passengers within physically constrained airport environments and minimizes disruptions to operations and wait times for passengers. Data from several of our member’s biometric pilots show that the time required for processes like bag drop and boarding is significantly reduced by using biometric technology. Faster passenger processing enables timely and efficient operations, for example, enabling more on-time departures and potentially reducing aircraft turn-around times.

**Safe and Contactless**

The COVID-19 pandemic has accelerated the consideration of biometrically enabled solutions that afford a contactless process that better promotes the health and safety of our employees and passengers. Continued improvements in technology and processes will help reduce verification times, remove repeated touch points and reduce passenger bottlenecks. Investments today in low-contact processes will make airlines and the traveling public more resilient to potential future health crises, reducing the health risk associated with close interactions between passengers and airline employees, and ease staffing concerns as travel resumes.

**Responsible Use**

As biometric technology continues to improve in speed, accuracy and reliability, our members are eager to adopt it in a responsible manner.

**Accuracy and Bias**

To realize our goals of improving security and the passenger experience, all technology and process variables in biometric verification must support accuracy and reliability. Disproportionate error rates across specific demographics – commonly referred to as “bias” – is counterproductive to our security goals and our commitment to passengers. The biometrics and computer vision industry in partnership with the Federal Government has made substantial gains in addressing bias and improving the accuracy of their algorithms. Airlines serve customers globally. We recognize the importance of and are committed to accuracy in algorithmic performance across all ethnicities and genders.

Inaccuracy rates, even at small percentages, have outsized impacts on populations as large and diverse as air travel passengers. False negatives and false positives in the air travel environment can severely undermine the government’s ability to fulfill its security mission, undercut carriers’ ability to confer benefits and facilitate the passenger experience, and tax operational resources for government and industry alike. High inaccuracy rates, therefore, do not scale for the security or airline business cases for biometrics.
With that in mind, we are encouraged by the tremendous technological strides in industry and commitment of our DHS partners to accuracy in facial matching. A 2019 National Institute of Standards and Technology (NIST) report on the performance of facial recognition algorithms across different demographic groups shows that the development of this technology is already highly accurate and improving. In both one-to-many and one-to-one facial matching, the most accurate high-performing algorithms achieved greater accuracy than humans, with low false positives and negatives across most demographic groups. Further, the current reality of masked passengers during the COVID-19 pandemic has spurred continued development and refinement of matching algorithms. Algorithms refined during the pandemic showed increased matching rates of masked passengers to the pre-pandemic algorithms, according to NIST. We applaud the industry’s rapid adaptability and overall commitment to continuous improvement.

Beyond the matching algorithm, there are additional variables in biometric verification that can affect accuracy and reliability. For example, we can control the quality of the image used for comparison by ensuring ideal conditions in lighting and image resolution. It is important to recognize that such complex technological tools can and should be adapted to the situations to which they are applied. As best practices emerge, our members are committed to adopting the most appropriate approach for different use cases, to deliver the optimal experience and service to the flying public.

Privacy and Data Security

Privacy and security of our passengers’ biometric data is of the utmost concern. Automated facial matching has privacy and data security protections built in to protect the biometric information in-transit and at-rest. As required by DHS when using DHS matching capability, photos taken for the purpose of automated facial matching are not retained and are purged by air carriers following their secure verification by DHS. Airline connections to secure, encrypted DHS systems for verification ensure passenger data is protected in-transit.

In addition, our members treat customers’ biometric information with the same care and diligence as other customer data. The airline industry is already well-equipped to protect the privacy of passenger data given its experience complying with global data protection regimes, such as the EU General Data Protection Regulation. Our members’ use cases are focused on the passenger travel journey.

Consent

Passengers must consent to leveraging their biometric information for automated facial matching. Although frequent fliers may be more familiar with biometric technology, non-frequent fliers often do not share the same awareness. The higher the passenger acceptance of automated facial matching, the stronger the realization of security, safety, and efficiency.

---


benefits. Therefore, we work with DHS to educate passengers on how the technology is being used and which personal data elements are being shared or stored.

On behalf of our members, we thank OSTP for providing the opportunity to submit information on the aviation use-case for biometrics. As explained in this response, security and facilitation is at the core of biometric use in the air travel environment. Biometric technology provides increased security for passengers while creating second-order effects of reducing health risk in travel and providing growth opportunities for operators. Our members work closely with DHS on improving the experience and protections for passengers. If you have any questions on this Biometrics RFI response, you can contact Lauren Beyer at [redacted].

Respectfully submitted,

Lauren Beyer
VP, Security and Facilitation